Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América

Facultad de Derecho y Ciencia Política
Unidad de Posgrado

De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010

TESIS

Para optar el Grado Académico de Magíster en Derecho con mención en Ciencias Penales

AUTOR

Jorge Martín PAREDES PÉREZ

ASESOR

Mg. Alexei Dante SÁENZ TORRES

Lima, Perú

2013

Para Ale.

Agradecimientos

Al Carlos Rios, gran amigo sanmarquino, por su invaluable apoyo

Al Coronel PNP Oscar Gonzales por su apoyo al facilitar la información de los casos investigados en la División de Alta Tecnología y por sus inteligentes sugerencias.

A Tomás Gálvez por el invaluable apoyo metodológico en la elaboración del presente trabajo.

A Alexei Saenz por sus importantes aportes.

ÍNDICE

INTRODUCCIÓN

La presente investigación titulada *De los delitos cometidos con el uso de sistemas informáticos: Problemas de tipificación de los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, durante el período 2009-2010,* desarrollará el problema principal referido a los problemas que se presentan al momento de la calificación del tipo penal de delito Informático, ya sea al formalizar la denuncia fiscal o al calificar dicha denuncia por el órgano jurisdiccional y su impunidad.

Igualmente, este trabajo se propone como objetivo principal demostrar que las conductas que emplean, utilizan o se basan en sistemas informáticos se encuentran deficiente e insuficientemente tipificadas y el ordenamiento jurídico resulta inadecuado para abarcar las principales manifestaciones que afectan importantes bienes jurídicos. Entre sus objetivos secundarios tenemos: *i)* determinar si existe una conducta a la que se pueda denominar en sentido estricto como "delito informático"; *ii)* Identificar cuáles son las limitaciones que existen en la tipificación del delito Informático al momento de formalizar la denuncia fiscal y/o en su calificación judicial; *iii)* demostrar que el delito informático se confunde en su

calificación con otros tipos penales, de tal forma que se estaría afectando el principio de legalidad y seguridad jurídica; *iv)* identificar cuáles son las manifestaciones de la criminalidad informática que no se encuentran tipificadas; *vi)* demostrar que la Ley 27309 no tipifica correctamente las afectaciones del patrimonio individual con el uso de sistemas informáticos, pues éste se encuentra tipificado en el artículo 183.3 del Código Penal, entre otros.

Como hipótesis general se ha planteado la siguiente: La inadecuada tipificación del delito informático y de las conductas que utilizan los sistemas informáticos, la existencia de conductas vinculadas a las nuevas tecnologías que teniendo relevancia penal no se encuentran tipificadas, y el uso de nueva tecnología en la comisión de los tipos penales tradicionales, son los factores que afectan la subsunción, formalización, procesamiento y eventual sanción –generando sensación de impunidad- de conductas que hacen uso de medios informáticos en la comisión de delitos en el Distrito Judicial de Lima, durante el período 2009-2010.

EL AUTOR

CAPÍTULO I

PLANTEAMIENTO METODOLÓGICO

1. DESCRIPCIÓN Y SELECCIÓN DEL PROBLEMA

1.1 Descripción de la realidad problemática materia de la investigación.

La criminalidad informática es la manifestación de nuevas conductas y manifestaciones criminales surgidas de la realidad delictiva al amparo de las tecnologías. Algunas de sus manifestaciones han sido tipificadas en nuestra legislación; en la reforma de 1991 del Código Penal, se incluyó en el capítulo de delitos contra el patrimonio individual la sustracción del espectro electro-magnético y el hurto mediante una transferencia no autorizada de fondos; en el 2000, se dictó la Ley Nº 27309 con el título de Ley de Delitos Informáticos; finalmente se introdujo conductas relacionadas con la promoción del turismo sexual infantil via la internet.

Las nuevas formas de criminalidad son producto del cambio que viene produciendose en las últimas décadas que ha producido cambios de tal magnitud como los efectuados por la revolución industrial del siglo XIX. La revolución tecnológica en la última década del siglo XX, impulsó el desarrollo de los sistemas informáticos en la cual la computadora dejó de ser una herramienta de oficina o empresa para invadir los hogares y abarcar todas las actividades y ocupaciones humanas; a ello se ha sumado la aparición de la internet que permite el acceso remoto a cualquier sistema informático demostrándonos que la idea de Bill Gates[1] - de ver el futuro conectado por una verdadera autopista de la información- es ya una realidad de la cual gozamos y nos beneficiamos.

Las ventajas ofrecidas por la tecnología facilitan la actividad criminal lesionando bienes jurídicos individuales o supraindividuales. Sin embargo, cuando aparecen las primeras manifestaciones de la nueva criminalidad informática se constata que los tipos penales clásicos, usualmente, carecen de la aptitud para incluir las conductas que surgen al amparo de las nuevas tecnologías por lo que la legislación penal contemporánea ha debido actualizarse a fin de incluir cabalmente estas nuevas agresiones.

Las nuevas tecnologías, en sistemas informáticos, nos han hecho ingresar de un mundo material, de cosas tangibles, a un mundo virtual, de cosas o elementos inmateriales, intangibles. El mundo virtual ha transformando todos los aspectos de nuestra vida y entre ellos al Derecho en todas sus manifestaciones no sólo en el uso de softwares legales o en documentos legales, archivos informatizados sino que se ha extendido a todas las áreas de la actividad humana; comercio, industria, sector financiero y bancario.

[1] Cfr. Gates, Bill. The path to the future. 1999. Avon Books. NY.

Empero, los problemas surgidos por la aparición y difusión de las nuevas tecnologías provenientes de la informática no han sido del todo resueltos por el ordenamiento jurídico a pesar del tipo penal del hurto agravado y la novísima ley de "delitos informáticos". Por el contrario, la dación de esta ley causa problemas concursales que afectan la eficacia de la norma. Esta situación estaría generando un clima de inseguridad entre los operadores de justicia para reprimir y tipificar correctamente las conductas delictivas que se realizan mediante el uso de sistemas informáticos.

Desde el plano dogmático se puede constatar que aún no se ha comprendido cabalmente el fenómeno criminal que utiliza nuevas tecnologías o sistemas informáticos por lo que las respuestas legislativas no resuelven los problemas planteados por ésta ni ofrecen una adecuada protección de bienes jurídicos. La falta de comprensión de las nuevas manifestaciones criminales ocasiona una legislación incompleta que no es suficiente para proteger correctamente los bienes jurídicos.

El problema de encontrar una adecuada tipificación o adecuación de las conductas a la norma legal estaría impidiendo la eficaz y adecuada represión de estas conductas. Asimismo, la comprensión cabal de los tipos penales que sancionan los actos de criminalidad informática permitirá la protección de la actividad empresarial y económica que se efectúen con la influencia de los sistemas informáticos.

En consecuencia, conforme a lo expuesto, podemos afirmar que existe una insuficiente tipificación que trae como consecuencia que múltiples conductas queden impunes; por lo que pretender forzar o ampliar el ámbito de aplicación de la ley penal afecta el principio de legalidad, además de que una inadecuada tipificación incide directa y negativamente en la probanza de las imputaciones.

1.2 Justificación e importancia de la investigación.

Ante la problemática descrita, la misma que además de grave es numerosa, es que hemos realizado la presente investigación propendiendo a la comprensión de la misma por parte de Jueces, Fiscales, miembros del Tribunal Constitucional y Abogados en general, con la finalidad de plantear algunas alternativas de solución al respecto.

En este sentido, la presente investigación se justifica plenamente, y a la fecha reviste especial importancia, ya que, como queda descrito, la problemática relativa al tema se muestra totalmente preocupante para todos los operadores vinculados al sistema de justicia y sobre todo, para las cada vez más numerosas víctimas de los delitos, quienes ven burlado su justo derecho a la adecuada protección de sus bienes jurídicos afectados por las conductas mencionadas.

Asimismo, es imperioso investigar en qué medida esta incertidumbre contribuye a la inseguridad y deslegitimación del sistema jurídico y qué factores determinan o inciden al mantenimiento de este estado de cosas; para ello he precisado previamente los fines y objetivos con cuya concreción se pretende contribuir al enriquecimiento de la teoría jurídica al respecto. A la vez que al determinar la

naturaleza jurídica de la criminalidad informática con el cual procuro contribuir con el logro de una eficaz protección de bienes jurídicos.

La presente investigación revela su importancia y se justifica también, debido al incremento de usuarios de las nuevas tecnologías en nuestro país que –a su vez- crea las condiciones para el aumento de las conductas ilícitas que se aprovechen de las facilidades que brindan estas nuevas tecnologías.

Creemos también que una adecuada administración del servicio de justicia contribuirá, a su vez, a una mejora de la paz social y en la calidad de vida de la población, contribuyendo a brindar seguridad jurídica y, como consecuencia de ello, una mejora sustancial en la percepción que la sociedad tiene de su sistema judicial.

1.3 Indagación sobre investigaciones preexistentes.

Se ha realizado la verificación de la relación de estudios de investigación realizadas sobre el presente tema en la biblioteca de la universidad, y no hemos podido encontrar trabajos a nivel de pregrado, ni de nivel de postgrado sobre la materia.

1.4 Delimitación de la investigación.

a. Delimitación espacial

La presente investigación se efectuará geográficamente en las Fiscalías del distrito judicial de Lima.

b. Delimitación temporal

La investigación comprenderá los años 2009 al 2010.

c. Delimitación cuantitativa.

La presente investigación se realizará según los términos de la muestra en las Fiscalías de los distritos judiciales de Lima, por cuanto consideramos que estos porcentajes nos dan una mayor seguridad en los resultados de la investigación.

2. FORMULACIÓN DEL PROBLEMA.

2.1 Problema principal

2.1.1 ¿En qué medida las conductas realizadas a través de los sistemas informáticos son abarcadas en los tipos penales en nuestro ordenamiento jurídico?

2.2 Problemas secundarios

2.2.1 ¿Qué problemas dogmáticos presenta la actual tipificación del delito informático?

2.2.2. ¿Cuál es el nivel de incidencia de las conductas realizadas a través de sistemas informáticos en la comisión de otros tipos penales ya tipificados en el Código Penal?

2.2.3. ¿La ley N° 27309 ofrece una protección adecuada de los bienes jurídicos afectados por el uso de sistemas informáticos?

2.2.4. ¿Cuál es el nivel de eficacia de la ley en la protección de bienes jurídicos que pueden ser afectados por la criminalidad informática?

2.2.5. ¿Cuáles son las dificultades que se presentan en la calificación e investigación de los delitos cometidos con el uso de los sistemas informáticos en nuestro actual ordenamiento jurídico penal?

3. OBJETIVOS Y FINALIDAD DE LA INVESTIGACIÓN.

3.1 Objetivos.

3.1.1 Objetivo general.

Demostrar que las conductas que emplean o se basan en sistemas informáticos se encuentran deficiente o inadecuadamente tipificadas y el ordenamiento jurídico resulta insuficiente para abarcar las principales manifestaciones que afectan importantes bienes jurídicos.

3.1.2 Objetivos específicos.

1. Determinar el nivel de eficacia del tipo penal denominado Delito Informático.

2. Determinar las conductas que se pueden denominar en sentido estricto como "delito informático".

3. Identificar las deficiencias en la tipificación actual.

4. Demostrar que el delito informático se confunde en su tipificación con otros tipos penales afectando el principio de legalidad.

5. Identificar las manifestaciones de la criminalidad informática que no se encuentran tipificadas.

6. Realizar el análisis dogmático analítico de la Ley 27309 que tipifica el delito de delito informático.

7. Proponer criterios para la adecuada tipificación de los delitos cometidos por medios informáticos.

3.2 Finalidad.

Con el logro de los objetivos anotados, se pretende proponer rigurosamente, ideas que permitan el conocimiento cabal del problema ocasionado con el uso de sistemas informáticos y proponer una respuesta legal eficiente para cautelar debidamente los principales bienes jurídicos con esta manifestación criminal.

4. HIPÓTESIS DE LA INVESTIGACIÓN

4.1 Hipótesis General

Debido a su desactualización, vacíos o defectos de la normatividad penal referida a la criminalidad informática, los tipos penales contenidos en nuestra legislación resultan insuficientes para abarcar adecuadamente las conductas realizadas con del uso de sistemas informatizados.

4.2 Hipótesis Derivada

(H-1) El empleo de tecnologías informatizadas por los agentes delictivos y el desconocimiento de estas tecnologías por operadores jurídicos y la ausencia de tecnologías adecuadas en las instituciones encargadas de la investigación de estos delitos generan grandes dificultades la debida calificación e investigación de estos delitos.

(H-2) La desactualización de nuestra normatividad legal determina la existencia de conductas no previstas en la legislación penal que requiere de una respuesta penal tales como: robo de identidad, comercialización de bases de datos o los ataques de saturación de páginas web o servidores del correo electrónico (Ataques DDoS)

(H-3) El uso de las nuevas tecnologías constituye un medio adecuado y sofisticado para la comisión de delitos tradicionales previstos en el Código Penal.

5. MARCO TEÓRICO.

Para el desarrollo de la presente investigación tendremos como modelos conceptuales generales: el carácter vinculante de la Constitución del Estado, la vigencia central del principio de legalidad, el principio de imputación necesaria y el bien jurídico tutelado por las conductas que utilizan sistemas informáticos.

Nuestro Estado de Derecho tiene a la Constitución Política como su norma fundamental. Cualquier desarrollo legislativo o interpretación de las normas se deben realizar a partir de esa norma fundamental.

El marco teórico se basa la Constitución que es la principal norma de nuestro ordenamiento jurídico y, por tanto, además de ser exigible, todas sus disposiciones regulan nuestro sistema normativo. Ello es fruto del reconocimiento que vivimos en un Estado social y democrático de derecho, por lo que hoy se concibe a la Constitución no sólo como un amplio espectro de sueños e ideales a alcanzar, sino como verdadera ley suprema que a través de sus normas vincula a todas las personas –naturales o jurídicas- e instituciones de un Estado[2].

La primacía de la Constitución en el sistema normativo ha sido reconocida por el Tribunal Constitucional peruano,[3] que de manera reiterada ha sostenido que: "La Constitución es una norma jurídica vinculante y los derechos que reconoce pueden ser directamente aplicados. Al respecto, este Tribunal ha declarado que la Constitución "(...) no es solo "una" norma, sino, en realidad, un "ordenamiento", que está integrado por el Preámbulo, sus disposiciones con numeración romana y arábica, así como por la Declaración sobre la Antártida que ella contiene. Toda ella comprende e integra el documento escrito denominado 'Constitución Política de la República del Perú' y, desde luego, toda ella posee fuerza normativa (...)". (Caso sesenta y cuatro Congresistas de la República contra los artículos 1°, 2°, 3.°, y la

[2] Cfr. Castillo Córdova, Luis, en *Comentarios al Código Procesal Constitucional,* Universidad de Piura, ARA Editores, 1ª. Edición, Lima octubre de 2004, pág. 43, afirma: "Si, como se ha argumentado, la Constitución peruana es norma jurídica fundamental, la consecuencia necesaria es que todo su contenido es normativo y vinculante. Esto, aplicado de las disposiciones de la Constitución que reconocen los derechos de la persona, significa que los derechos constitucionales vinculan tanto al poder político como a los particulares. Es decir, que los derechos constitucionales son categorías jurídicas plenamente vigentes y que deben ser respetadas por sus destinatarios." En tal sentido, no le falta razón al profesor Santa Cruz, Julio, en sus *Notas sobre Interpretación y Dogmática en la aplicación de la ley penal,* Revista 4 de la Academia de la Magistratura, Lima 2000, cuando afirma que ..."en el Estado constitucional la ley carece de autonomía porque siempre habrá de rendir cuenta ante la instancia superior de la Constitución."

[3] Por todas y a manera de ejemplo véase la STC Exp. 008-2005-PI/TC – Juan José Gorriti y otros.

primera y segunda disposición final y transitoria de la Ley N.° 26285, Exp. N.° 005-2003-AI/TC, fundamento 21)."

El principio de legalidad surge como fundamento de la actividad persecutoria. En buena cuenta a partir de este principio se desprenden importantes consecuencias como el principio de imputación necesaria que tienen relación directa con el derecho de defensa. El principio de legalidad se condensa en la célebre fórmula enunciada en latín "*nullum crimen, nulla poena sine lege*",[4]

De otro lado, como se sabe, el derecho penal moderno se basa, mayoritariamente, en la protección de bienes jurídicos. Por lo tanto, resulta indispensable para esta investigación determinar cuál es el bien jurídico o cuáles son los bienes afectados por las conductas que utilizan los sistemas informáticos. Establecer si éstos ya cuentan con protección en el ordenamiento penal o si la nueva criminalidad ha generado la aparición de un nuevo bien.

6. METODOLOGÍA DE LA INVESTIGACIÓN

6.1 Tipo y nivel de investigación

- ***Tipo de investigación:*** Causal explicativa.
- ***Nivel de investigación:*** Descriptivo, Explicativa y Comparativo.

6.2 Método y Diseño de la investigación

- ***Método de la investigación:*** Descriptivo, Dogmático, Inductivo, Deductivo, Histórico y Analítico.
- ***Diseño de la investigación:*** Descriptivo comparativo.

[4] Este principio fue incluido en la "Declaración de derechos del hombre y del ciudadano" de 1789 y un poco antes en la declaración norteamericana de Filadelfia de 1774.

6.3 Universo, población y muestra

a. Universo

Fiscalías y Juzgados de los distritos judiciales de Lima, Lima Norte y Callao durante el período 2009-2010.

b. Población

Procesos penales sobre Delito Informático, operadores de derecho y especialistas.

c. Muestra

30% del total de denuncias fiscales y procesos penales sobre delito Informático que se siguen ante los órganos jurisdiccionales mencionados, entrevistas y encuestas con magistrados (12 en total) y especialistas en el tema (6 en total).

6.4 Instrumentos y Fuentes de Recolección de Datos

a. Técnicas:

Documental

Entrevistas

Cuestionarios

b. Instrumentos:

Se utilizará como instrumentos: Fichas bibliográficas, Encuestas, Guías para entrevistas y análisis de expedientes.

c. Fuentes:

Bibliográficas

Normas

Tratados

Docentes/Especialistas.

6.5 Técnica de recolección de datos.

La recolección de datos está dado por:

a) Fichaje de bibliografía y de resumen que se obtengan sobre el tema con carácter general y especializada, los que obtendremos apersonándonos a la biblioteca de la Facultad y de los que adquiramos por la compra o expedición de copias por nuestra cuenta.
b) Análisis documental respecto de la doctrina a considerar en la presente investigación, así como de las teorías y de las normas relacionadas al tema, para lo cual nos valdremos de las fichas que se hayan obtenido.
c) Estudio de casos relacionados con el tema de investigación, escogidos aleatoriamente, para lo cual nos constituiremos en los diferentes juzgados y salas penales de los distritos judiciales mencionados.
d) Encuestas que se elaborarán en función del problema planteado, las hipótesis y variables identificadas, precisando las preguntas más adecuadas en un cuestionario, siguiendo criterios científicos, y para la toma de las muestras tendremos que apersonarnos a los diferentes juzgados y salas penales de los distritos judiciales mencionados.
e) Entrevistas con los distintos operadores de derecho que laboran en las sedes judiciales mencionados, de conformidad a los porcentajes y distribución planteados con anterioridad, para lo cual nos constituiremos en dichos lugares.

6.6 Procesamiento y análisis de datos.

Obtenidos los datos de la investigación, se procederá a su procesamiento y análisis del siguiente modo:

a. Selección y representación de variables, es decir, se seleccionarán las respuestas de las encuestas y entrevistas de acuerdo a las variables formuladas.
b. Matriz tripartita de datos, en la que se almacenarán provisionalmente la información obtenida y que previamente ha sido seleccionada.
c. Pruebas estadísticas en función de las diversas técnicas: tablas cruzadas, distribución de frecuencias, asociación y correlación entre variables.
d. Uso del procesador sistematizado que nos facilitarán en la labor estadística: básicamente aquellos contenidos en el Programa Windows 2007.

CAPÍTULO II

DESARROLLO DE LAS INSTITUCIONES JURÍDICAS COMPRENDIDAS EN EL MARCO TEÓRICO

1. MARCO HISTÓRICO

1.1 Evolución legislativa de los delitos cometidos a través de medios informáticos.

1.1.1. Evolución legislativa del hurto telemático

En los proyectos prelegislativos que culminaron con la promulgación del Código Penal en 1991 no aparece el hurto telemático como agravante del hurto aunque desde el proyecto de 1986 la definición de la cosa mueble incluye a bienes inmateriales con valor económico como las energías o el agua.

Como se puede apreciar en el texto final del Código Penal de 1991 se establece dos importantes innovaciones que incluyen los conductas que utilizan los sistemas informáticos; el concepto de cosa mueble se extiende a bienes incorpóreos con valor económico y, concretamente, el hurto telemático.

Proyecto de 1986[5]

> **187 Hurto tipo base**
> El que se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, para aprovecharse de él, sustrayéndolo del lugar donde se encuentra…
>
> Se equipara a bien mueble la energía eléctrica, el gas, el agua y cualquier otro elemento similar que tenga valor económico.

188 agravantes

No incluye hurto telemático

Proyecto de 1991[6]

> **185 Hurto tipo base**
> El que, para obtener provecho, se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra…
>
> Se equiparan a bien mueble la energía eléctrica, el gas, el agua y cualquier otra energía o elemento que tenga valor económico

186 agravantes

No incluye el hurto telemático.

[5] Ministerio de Justicia. Ed mimeografiada, Lima 1986
[6] El Peruano, 20 de enero de 1991.

Código Penal de 1991[7]

185 Hurto tipo base
El que, para obtener provecho, se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra…

Se equiparan a bien mueble la energía eléctrica, el gas, el agua y cualquier otra energía o elemento que tenga valor económico, así como el espectro electromagnético.

186 agravante
pena privativa de libertad no menor de dos ni mayor de cuatro años
(…)
Si el agente usa sistemas de transferencia electrónica de fondos, de la telemática en general, o viola el empleo de claves secretas será reprimido con pena privativa de libertad no menor de tres años ni mayor de seis años y con ciento ochenta a trescientos sesenticinco días-multa

Ley Nº 26319[8]

186 agravantes
pena privativa de libertad no menor de tres ni mayor de seis años(…)

La pena será no menor de cuatro ni mayor de ocho años (…)

3. Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.

La pena será no menor de ocho ni mayor de quince años (…)

1.1.2. La promoción de turismo sexual infantil a través de medios informáticos.

La Ley Nº 28251 (08.06.2004) incorporó el Artículo 181º- A el cual fue modificado por la Segunda Disposición final de la Ley Nº 29408 (18.09.2009).

[7] El Peruano, 8 de abril de 1991.
[8] El Peruano 27 de mayo de 1994

Artículo 181-A.- Turismo sexual comercial infantil y adolescente en ámbito de turismo.
El que promueve, publicita, favorece o facilita la explotación sexual comercial en el ámbito del turismo, a través de cualquier medio escrito, folleto, impreso, visual, audible, electrónico, magnético o a través de internet, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de catorce (14) y menos de dieciocho (18) años de edad será reprimido con pena privativa de libertad no menor de cuatro (4) mi mayor de ocho (8) años.

Si la víctima es menor de catorce años, el agente, será reprimido con pena privativa de libertad no menor de seis (6) ni mayor de ocho (8) años.

El agente también será sancionado con inhabilitación conforme al artículo 36º incisos 1,2, 4 y 5.

Será no menor de ocho (8) ni mayor de diez (10) años de pena privativa de la libertad cuando ha sido cometido por autoridad pública, sus ascendientes, maestro o persona que ha tenido a su cuidado por cualquier título a la víctima.

El Artículo 182º-A fue Incorporado por el Artículo 2º de la Ley Nº 28251 (08.062004).

Artículo 182º-A.- Publicación en los medios de comunicación sobre delitos de libertad sexual a menores.
Los gerentes o responsables de las publicaciones o ediciones a transmitirse a través de los medios de comunicación masivos que publiciten la prostitución infantil, el turismo sexual infantil o la trata de menores de dieciocho años de edad serán reprimidos con pena privativa de la libertad no menor de dos ni mayor de seis años.
El agente también será sancionado con inhabilitación conforme al inciso 4 del artículo 36º y con trescientos sesenta días multa.

El Artículo 183º-A fue Incorporado por el artículo 2º Ley Nº 27459 (26.05.2001) y modificado por el artículo 1º Ley Nº 28251 (08.06.2004).

Artículo 183º A.- Pornografía Infantil
El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio incluido la internet, objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no

menor de cuatro ni mayor de seis años y con ciento veinte a trescientos días multa.
Cuando el menor tenga menos de catorce años de edad la pena será no menor de seis ni mayor de ocho años y con ciento cincuenta a trescientos sesenta y cinco días multa.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173º, o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil la pena privativa de libertad será no menor de ocho ni mayor de doce años.
De ser el caso, el agente será inhabilitado conforme al artículo 36º, incisos 1, 2, 4 y 5.

1.1.3. La incorporación de los delitos informáticos al Código Penal. Evolución legislativa de la Ley Nº 27309.

Posteriormente, en el año 2000, con el excesivo nombre, "Ley que incorpora los delitos informáticos al Código Penal" intentó definir conductas concretas que utilizan o afectan los sistemas informáticos.

Proyecto Nº 5071

Proyecto de Ley de Delitos Informáticos

> **Artículo 208-A.-** El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.
>
> **Artículo 208-B.-** El que indebidamente, interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadoras o los datos contenidas en la misma, en la base, sistema o red será reprimido con pena privativa de libertad no mayor de dos años.

Ley Nº 27309[9]

[9] El Peruano 17 de julio de 2000.

CAPITULO X

Artículo 207-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Artículo 207-C.- En los casos de los artículos 207º-A y 207º- B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo
2. El agente pone en peligro la seguridad nacional.

1.2. Normas legales que regulan las manifestaciones de las nuevas tecnologías.

Adicionalmete a la reseña legislativa anotada, referida al ámbito penal, a partir 1991, coincidiendo con la promulgación del Código Penal, se dictaron diversas normas dirigidas a regular los aspectos legales de los documentos elaborados por procesos tecnológicos e informáticos, sus sistemas de seguridad, los archivos informatizados, el fedatario informático y, por otro lado, se establecieron medidas preventivas para evitar la difusión de la pornografía infantil.

A continuación una breve reseña de las normas relativas a la regulación legal de los procesos y productos informáticos:

- **CONSTITUCIÓN POLÍTICA DEL PERÚ.** (1979)

  Derechos Fundamentales de las personas.

  Artículo 2. Toda persona tiene derecho:

  numeral 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

- **DECRETO LEGISLATIVO Nº 681** (14-10-91)

> Regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto a la producida por procedimientos informáticos en computadoras.

En esta primera norma se regula los documentos procesados con nuevas tecnologías y por medios informáticos. Entre ellas se define a la microforma como cualquier imagen reducida y condensada, o compactada, o digitalizada de un documento. Se incluye también a los documentos producidos por procedimientos informáticos y a los elaborados a través de procedimientos técnicos de microfilmación. Es de recordar, que antes de la introducción de medios informáticos se realizaba la micorfilmación por procedimientos fotográficos que reducían y compactaban documentos.

El aspecto central del concepto de microforma se encuentra en que el medio tecnológico premita que la imagen se conserve, pueda ser vista o leída y ser reproducida en copias impresas, esencialmente iguales al documento original.

Asimismo, esta norma regula la actuación de los Fedatarios Públicos y particulares como depositarios de la fe pública, pues su actuación da fe de la elaboración e idoneidad de los documentos electrónicos.

Las microformas y sus microduplicados elaborados de acuerdo a la regulación legal mantienen sus efectos legales. Y pueden sustituir a los expedientes, idoneidad de los microformas. Se considera fecha cierta la fecha en que el documento fue micrograbado que conste en el acta de cierre.

Los Notarios públicos o fedatarios dan fe de las copias de los documentos microfilmados o microporcesados como copia autentica.

Finalmente, en el artículo 19 se establece, específicamente, la protección penal de los documentos microfilmados a través de los delitos contra la fe pública.

Artículo 19º.- La falsificación, y la adulteración de microformas, microduplicados y microcopias, sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe pública, conforme a las normas pertinentes del Código Penal.

- **DECRETO SUPREMO Nº 009-92-JUS** (27.06.92) Reglamento del Decreto Legislativo Nº 681, sobre el uso de tecnologías de avanzada en materia de archivos de las empresas.

En este Reglamento se precisa la actuación de los Fedatarios informáticos, tanto los adscritos a la Notaría Públicas y los fedatarios particulares que ofrecen sus servicios de manera privada los cuales deberán mantener sus archivos que garanticen la conservación de este tipo de documentos. Asimismo, se regulan los efectos legales documentos autenticados con firma informática.

- **DECRETO SUPREMO Nº 070-2011-PCM**.
  Decreto Supremo que modifica el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo Nº 681 y ampliatorias

Establece las presunciones legales de las comunicaciones legales a las comunicaciones electrónicas generadas por la administración pública que hayan contado con el sello web trust y su posterior reemplazo por los certificados generados por RENIEC.

Tambien se establece que el INDECOPI es la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica – IOFE-. Autogenera el Certificado Raíz y los subsiguientes que correspondan.

- **DECRETO SUPREMO Nº 001-2000-JUS (26-03-2000)** reglamento sobre la aplicación de las normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información a entidades públicas y privadas.

Se precisa que los documentos obtenidos por medios tecnológicos deben mantener la seguridad e integridad de datos que garanticen su inalterabilidad en la que se incluye a la firma informática forma parte de la seguridad de los datos informatizados. De acueros a este Decreto Supremo la firma informática o digital será utilizada para autenticar los procesos de micrograbación de los archivos.

En el artículo 6 de esta norma se establece que microformas archivadas por las entidades públicas, obtenidos conforme a las normas del Decreto Legislativo Nº 681, tienen pleno valor probatorio y efecto legal para su uso en procedimientos administrativos y para su transmisión telemática.

- **Ley Nº 27269.** (28.05.00)
  Ley de Firmas y Certificados Digitales

Esta Ley regula el uso de la firma electrónica y le otorga la misma validez y eficacia jurídica que el de una firma manuscrita u otra análoga que acredite la manifestación de voluntad entendido como la extensión de la personalidad signos que identifican a una persona.

La firma electrónica es cualquier símbolo que utilice medios electrónicos con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

La firma electrónica vincula e identifica al firmante y garantiza la autenticación e integridad de los documentos electrónicos.

Por otro lado, se precisa que la firma digital es la firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único. Esta firma se forma con la asociación de una clave privada y una clave pública que se relacionan matemáticamente.

El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual se vincula con un par de claves de una persona determinada.

- **DECRETO SUPREMO Nº 052-2008 PCM (19/07/08)**
  Reglamento de Ley de firmas y certificados digitales.

Establece los requisitos para la validez jurídica de la firma digital en reemplazo de la firma manuscrita. Los documentos electrónicos serán suscritos con una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica ya que ésta tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. Presunción de veracidad del documento cuando se utilizó la clave privada del suscriptor.

Estos documentos electrónicos firmados digitalmente serán admitidos como prueba en los procesos judiciales y/o procedimientos administrativos.

En caso de controversia sobre la validez de la firma digital, el Juez podrá solicitar a la Autoridad Administrativa Competente el nombramiento de un perito especializado en firmas digitales, sin perjuicio de lo dispuesto por los artículos 252, 264 y 268 del Código Procesal Civil.

Las normas del Decreto Legislativo N° 681 y su Reglamento regulan las características de un documento firmado digitalmente que se ha convertido en una microforma o microarchivo.

Se crea la Infraestructura "Oficial de Firma Electrónica" constituida por:

a) El conjunto de firmas digitales, certificados digitales y documentos electrónicos generados bajo la Infraestructura Oficial de Firma Electrónica.
b) Las políticas y declaraciones de prácticas de los Prestadores de Servicios de Certificación Digital, basadas en estándares internacionales o compatibles con los internacionalmente vigentes, que aseguren la interoperabilidad entre dominios y las funciones exigidas, conforme a lo establecido por la Autoridad Administrativa Competente.
c) El software, el hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales comprendidas en los estándares señalados en el literal b).
d) El sistema de gestión que permita el mantenimiento de las condiciones señaladas en los incisos anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.
e) La Autoridad Administrativa Competente, así como los Prestadores de Servicios de Certificación Digital acreditados o reconocidos.

Criptografía Asimétrica.- Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente

relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (clave pública). Las claves están matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.

En el glosario de esta norma se define al "**documento**" como "cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado."

También se incluye la definición de "**documento electrónico**" Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.

Por otro lado, el "domicilio electrónico" es la dirección electrónica que constituye la residencia habitual de una persona dentro de un Sistema de Intermediación Digital y en el caso de una persona jurídica el domicilio electrónico se asocia al de sus integrantes.

También se considera que el expediente electrónico se encuentra conformado por los trámites o procedimientos administrativos en la entidad que agrupa una serie de documentos o anexos identificados como archivos, sobre los cuales interactúan

los usuarios internos o externos a la entidad que tengan los perfiles de accesos o permisos autorizados.

La "**Infraestructura Oficial de Firma Electrónica**" es el sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de la integridad de los documentos electrónicos y la identidad de su autor.

Se definen los "**medios telemáticos**" al conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

El **certificado WebTrust** es una certificación otorgada a prestadores de servicios de certificación digital - PSC, específicamente a las Entidades Certificadoras - EC, que de manera consistente cumplen con estándares establecidos por el Instituto Canadiense de Contadores Colegiados (CICA por sus siglas en inglés - ver Cica.ca) y el Instituto Americano de Contadores Públicos Colegiados (AICPA). Los estándares mencionados se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio.

- **Ley Nº 27419** (06.02.00)

  Modifica al Código Procesal Civil para permitir la notificación de determinados actos procesales a través de correos electrónicos.

- **Ley Nº 28493** (12.04.05)
  Regula el correo electrónico comercial no solicitado. (spam)

  Establece una compensación económica de 1% de UIT a 3% de UIT por cada spam.

Esta norma regula la difusión de correos electrónicos comerciales y establece sanciones por difundir correos electrónicos comerciales no autorizados. Un correo electrónico comercial deberá ser identificado como tal y deberá contener una dirección de correo válida para que el usuario pueda notificar su decisión de no recibir correos publicitarios.

Se considera "**Correo electrónico**" a todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico.

El **Correo electrónico comercial** es todo correo electrónico que contenga información comercial publicitaria o promocional de bienes y servicios de una empresa, organización, persona o cualquier otra con fines lucrativos.

La Dirección de correo electrónico se identifica por la serie de caracteres utilizada para identificar el origen o el destino de un correo electrónico.

Se entiende que un correo electrónico comercial no solicitado es ilegal (spam) cuando no cumpla con los requisitos establecidos en el artículo 5° de la esta Ley o contenga información falsa del remitente, del asunto o cuando se envíe a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos (2) días.

La sanción se aplica cuando el usuario cuando reciba el correo electrónico comercial a pesar de haber expresado su rechazo mediante el reenvío señalado en el literal d) del artículo 3° de la Ley.

- **Ley Nº 28119** (13-12-03)
  Ley que prohíbe el acceso de menores de edad a páginas Web de contenido pornográfico.
  Modificado por la Ley N° 29139 (01.12.2007)
  Art 2 instalación de navegadores gratuitos, la adquisición de software especiales de filtro y bloqueo o a través de cualquier otro medio que tenga como efecto impedir la visualización.

Como un mecanismo de protección a los menores que utilizan las **cabinas de internet públicas** y como prevención del delito de pornografía infantil se dispone la instalación de software especiales o filtros que impidan a los menores de edad usuarios no puedan acceder a páginas web, canales de conversación o cualquier otra forma de comunicación en red de "contenido pornográfica u otras formas reñidas con la moral o el pudor, que atenten contra su integridad o afecten su intimidad personal y/o familiar".

Se encarga las municipalidades ejercer la fiscalización y control de los locales que conducen cabinas de internet respecto al cumplimiento de las medidas de control y le aplican las sanciones correspondientes.

- **Ley Nº 29733** (03/07/2011)
  Ley de Protección de Datos Personales

Es una ley marco que define los datos personales tratados informáticamente que se encuentran almacenados en bases de datos públicos o privados.

Se crea la **Autoridad Nacional de Protección de Datos Personales** con potestad sancionadora de las infracciones que se cometan, establece las multas a imponer y puede realizar la cobranza coactiva.

Se establecen las Infracciones a la Ley de Protección de Datos a toda acción u omisión que contravenga o incumpla alguna de las disposiciones contenidas en

esta Ley o en su reglamento. Las infracciones se califican como leves, graves y muy graves.

La Ley define el concepto de "**Banco de datos personales**" al "conjunto organizado de datos personales, automatizado o no", independientemente del soporte que lo contengan.

Los "**datos personales**" son "toda información sobre una persona natural que la identifica o la hace identificable" mientras que los "datos sensibles" se refieren a los datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual. "

- **DS Nº 003-2013-JUS** (21/03/13)
  Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.

Contiene un glosario de definiciones que contiene la Ley Nº 299733. Entre ellas destacan:

- Sobre los datos se define y diferencia a los "datos personales", "datos personales relacionados con la salud" y "datos sensibles".
- Los "datos sensibles" son "características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponde a la esfera más íntima"

La ley y su reglamento no serán aplicables cuando los datos sean utilizados con:

- Fines personales o domésticos.

- Para el uso de la administración pública que tengan como objeto la defensa nacional, seguridad pública o la investigación y represión del delito.

Se exige el consentimiento expreso e inequívoco y por escrito de titular del "dato sensible" para poder tratarlo informáticamente. Entre las formas de dar consentimiento o manifestar la voluntad del titular comprenden la firma electrónica o mediante un "clic".

Se entiende exonerada del consentimiento del titular cuando los datos se encuentran en fuentes accesibles al público como los contenidos en medios de comunicación, guías telefónicas, listas de colegios profesionales o Registros Públicos.

Los sistemas informáticos que manejen bancos de datos personales deberán instalar medidas de seguridad que controlen el acceso a la base e identifiquen al usuario. Además que permitan realizar la trazabilidad del acceso o uso de las bases.

El Registro de Banco de Datos, creado por la Ley Nº 29733, tiene carácter público

- **Ley Nº 29985**

  Ley que regula las características básicas del dinero electrónico.

Regula la emisión de dinero electrónico y de las empresas autorizadas a emitirlos.

Emisión, reconversión a efectivo, transferencias y como medio de pago.

Características del dinero electrónico:

- Medio de pago y efecto cancelatorio.
- Almacenado en soporte electrónico.
- Convertible a dinero en efectivo.
- Emitido por igual valor al dinero depositado.

Esta norma facilita la transferencia de dinero electrónico entre personas (P2P), empresas (G2P) o incluso con entidades estatales (G2P) . Solo es necesario contar con un teléfono móvil (que se convierte en una billetera electrónica) para recibir o transferir el dinero. El monto de las transferencias pueden fluctuar entre 3 soles a 3,700 soles.

Las empresas operadoras de dinero móvil o electrónico se denominan Empresas Emisoras de Dinero Electrónico (EEDE) y deberán inscribirse en el registro de la SBS. La función central es la emisión del dinero electrónico con respaldo al dinero depositado por los usuarios en los "puntos de recaudación".

2. DE LAS CONDUCTAS RELACIONADAS CON LA CRIMINALIDAD INFORMATICA

2.1. De la revolución industrial a la revolución informática.

La revolución tecnológica que comenzó en la segunda mitad del siglo XX es solo comparable, por sus impactos socio económico y sociales, a los producidos por la revolución industrial del siglo XIX. En efecto, la revolución industrial que se inició en la Inglaterra victoriana con la aparición de la máquina que sustituyó el trabajo manual, por un lado, y por otro lado, el ferrocarril y el telégrafo fueron los nuevos medio de comunicación que acortaron las distancias y permitió, por primera vez, la conexión casi instantánea entre personas que se encontraban en ultramar produjo profundos e irreversibles cambios en todos los aspectos de la vida cotidiana. Similar impacto causó la aparición de la informática que ya se puede hablar con propiedad de la "revolución informática" con la creación de la computadora y luego la Internet que permitió su interconexión infinita en los

sistemas informáticos. Estos inventos fueron posibles gracias a la creación del micro chip y del código binario que representa en un sistema de dos dígitos de 0 y 1 textos, imágenes o instrucciones a la computadora o sistemas de telecomunicación. Estos inventos crearon una nueva forma de comunicarse o relacionarse interpersonalmente ocasionando con importantes impactos en el derecho. La economía, las relaciones sociales, la educación y entretenimiento. Estos adelantos tecnológicos incluso han modificado la manera de conectarnos o comunicarnos con los demás está siendo socavada por nuevas prácticas (compras on-line, chats, e-mail, educación a distancia, foros de discusión.

La revolución informática o tecnológica es impulsada por la informática[10], Los sistemas informáticos registran y procesan automáticamente información, de cualquier índole, en tres tareas básicas: i) entrada, ii) procesamiento o tratamiento de información y iii) salida o transmisión de resultados.

La super autopista que conecta al mundo es la internet, a la cual nos unimos desde nuestro propio ordenador, gracias al uso combinado de las computadoras y las redes de comunicación con una simple conexión o un click del mouse. Una vez conectados ingresamos al espacio virtual, digital sin controles ni seguridad en el cual acechan, anonimamente, miles de piratas informáticos que esperan obtener la información personal, bancaria o incluso ingresar a nuestros hogares u oficinas espiandonos. Vivimos, desde hace un par de décadas en una aldea global o un mundo virtual sin control ni reglas en el que somos más vulnerables que en el mundo físico o real quizá porque la humanidad en miles de años aprendió a resguardarse de las amenazas físicas colocando medios físicos de protección. Al cerrar y asegurar la puerta de nuestras casas estamos seguros que nadie podrá ingresar. Sin embargo, aún no somos totalmente concientes respecto a la

[10] La "informática" es un término acuñado en 1957 por Karl Stainbuch[10] en su trabajo denominado "informática: procesamiento automático de información".

vulnerabilidad en el mundo virtual. Incluso en el interior de nuestros hogares u oficinas podemos tener un intruso sin que nos percatemos de ello pues un programa espía puede tomar control de la computadora y copiar la información, espiar nuestros movimientos, etc.

De esta manera, la tecnología ha creado un mundo virtual o el ciberespacio[11] distinto al mundo material conocido, en la revolución tecnológica o informática no sólo trae beneficios o únicamente nos facilite los aspectos de cotidianos ya que uno de sus caracterísitacas principales es el anonimato y la comunicación o interelación transfronteriza. El cyberespacio es ocupado por delincuentes que se aprovechan de los adelantos tecnológicos para obtener beneficios afectando bienes jurídicos con el agravante que las conductas disvaliosas realizadas en el "virtual" gozan de cierta impunidad gracias al anomimato y por el hecho que las comunicaciones informáticas son transfonterizas.

2.2. El impacto de las nuevas tecnologías en el Derecho penal. El ciberespacio o comunidad virtual.

Hoy nadie duda de que el mundo sufre los efectos de la revolución tecnológica producida a fines del siglo XX. Y es que desde el primer correo electrónico enviado el 29 de octubre de 1969 en la Universidad de Stanford – California, se ratificó el apogeo de la tecnología y señaló el cambio irreversible en la manera de comunicarse.

La tecnología, pues, ha modificado también en definitiva y sustancialmente las relaciones interpersonales. Los seres humanos compartimos un nuevo tipo de comunidad denominada ciberespacio; una comunidad virtual compuesto por

[11] De acuerdo al profesor Pérez Luño, "El ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada." Pérez Luño, Antonio Enrique. *Impactos Sociales y Jurídicos de internet*. En www.argumentos.us.es/numero1. En el mismo sentido Corcoy p. 145 quien resalta los aspectos negativos de la tecnológia.

vecinos anónimos integrados, a nivel mundial, desde su computador. En la nueva sociedad es cada vez más usual la comunicación o interrelación personal a través de medios electrónicos creando relaciones *on line* en el espacio virtual o ciberespacio. La vida moderna, "*on line*", desarrolla relaciones anónimas a través de la pantalla del ordenador para comprar, vender, ofrecer servicios, educarse o incluso para enamorarse y hasta se envían las peticiones e intenciones para el pozo de los deseos de Santa Rosa de Lima por internet. La primera Santa de América tiene además una cuenta de facebook. En estos momentos podríamos decir que, si bien es cierto el hombre sigue siendo un ser social, hoy es "un ser cibersocial", pues tras la máquina puede estar una persona absolutamente tímida o de difícil de comunicarse con los demás, pero a través del computador puede superar tal debilidad o aparentar ser otra persona.

La sociedad virtual está compuesta de bites, impulsos eléctricos, en los cuales se almacenan, en un código binario, información con valor económico o dinero virtual, se registran transacciones económicas, se desarrolla el comercio electrónico, se almacena o transfiere información sobre seguridad nacional o relativa a secretos industriales. En este mundo virtual –donde prácticamente nada le es ajeno- se realiza la mayoría de las transferencias de bienes o dinero o circula información con valor económico y por ello no es extraño que con el desarrollo de la tecnología los delincuentes hayan ingresado al mundo cibernético para obtener sus ganancias ilícitas.

Los sistemas informatizados almacenan y manejan información o data. La información o los datos almacenados constituyen el corazón de un sistema informático. El tratamiento electrónico de la información ha devenido en un elemento esencial en la sociedad actual alcanzando la calidad de "un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de

autonomía y objeto del tráfico"[12]. La información resulta más útil y valiosa cuando puede ser recuperada rápidamente a través de la interconexión de las bases de datos conocidas como la gran autopista de la información a través de la cual circulan cada vez más datos de personas y empresas.

El inesperado desarrollo de la Internet, la supercarretera de la información, en la última década del siglo XX convirtió a cada usuario en una terminal del sistema informatico al concetarse desde su casa y originó un espacio sin control que facilitó la proliferación de conductas ilícitas o la circulación de material nocivo. Sin embargo, la internet es visitado constantemente por toda clase de delincuentes quienes se aprovechan de los medios tecnológicos o de la informática para cometer las más variadas actividades criminales. El problema surge cuando una conducta específica no se encuentra regulada o un hecho concreto no está tipificado como delito y se constata una laguna de punibilidad. Entonces, desde la perspectiva del derecho penal se pregunta si es necesario proteger al nuevo bien jurídico y si resulta indispensable sancionar esta conducta.

Pérez Luño[13], acertadamente, define al internet como todas las grandes conquistas cientificas y tecnológicas "una realidad ambivalente" que nos ofrece innegables e irrenunciable beneficios pero que también facilita la actuación de los criminales en la red.

Los cambios sociales promovidos por la difusión de la tecnología impulsaron, a su vez, la reforma legislativa como un imperativo para proteger nuevos bienes jurídicos o adecuar la legislación para evitar las posibles lagunas de impunidad. Se debe tener presente que el impacto de la explosión tecnológica es un problema que la política criminal conoce sobradamente. La técnica siempre es un arma y cada

[12] Cfr. Gutierrez Frances, Mariluz. *Delincuencia económica e informática en el nuevo Derecho Penal.* España, p.251.
[13] Cfr. Pérez Luño, Antonio Enrique. *Impactos Sociales y Jurídicos de internet ...*

avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen.

2.3. El silbato del Capitán Crunch anuncia el arribo de la criminalidad tecnológica. La criminalidad informática o la cyber criminalidad.

Al inicio de los 70s la compañía de cerales "Capitán Crunch" regaló un silbato sin presagiar que los 2600 Hz que emitía sería utilizado para defraudar a la compañía telefónica. De manera circunstancial un amigo ciego del ingeniero John T Draper[14] le comentó que el tono que producía ese juguete era similar al tono de larga distancia de las centrales telefónicas de la AT&T con lo cual al soplar el silbato se obtenían llamadas de larga distancia gratis.

Con este descubrimiento, Draper prepararó la "***blue box***" un dispositivo más elaborado que emitía el tono de 2600 Hz y contaba con un teclado para efectuar las llamadas defraudando a AT&T. Este primera tecnología afectaban la frecuencia de audio que hacía funcionUn joven ar las centrales de telefonía para conseguir llamadas telefónicas era desarrollada por los "***phreakers***" o los piratas telefónicos quienes manejaban y manipulaban redes o sistemas telefónicas paradójicamente impulsó el desarrollo de la incipiente tecnología informática.

Al inicio de la era informática se creó una subcultura de hackers[15] integrada por jóvenes interesados en la electrónica o la tecnología en general que se reunieron en el *Homebew Computer Club* (Club informático casero) en el cual se intercambiaba

[14] http://es.wikiopedia.org/wiki/John_Draper. Draper, a consecuencia de la publicación de un artículo periodístico publicado en la Revista *Esquire* por Ron Rosenbaum en octubre de1971 "*Secrets of the little blue box*" en el cual se reveló la forma como se manipulaba las centrales telefónica provocó una enorme represión contra los *phreakers* en el cual la posesión de una blue box podía acarrear una sanción hasta dos años de cárcel. Como cololario de esta razia, Draper fue condenado a por la comisión del delito federal de fraude a la empresa telefónica por lo cual estuvo detenido por 4 meses.

[15] Isaacson, Walter. Steve Jobs. La biografía. Ed. Debate. Bs. As. 2011. p. 72 y ss.

información sobre los últimos avances tecnológicos guiados por la ética hacker que promovía la difusión gratuita de la información. Sin embargo, Bill Gates y Paul Allen cuando constatan que su software BASIC es compartido y copiado sin recibir ningún pago envía una carta al club quejándose de la piratería de sus compañeros. La información que se difundía en estas reuniones llevó al desarrollo de la primera computadora personal el creador de Apple. Steve Jobs, el futuro fundador de Apple, tampoco creía que el desarrollo tecnológico debería ser gratuito.

Las redes de telefonía que fueron las primeras redes de comunicación anterior a la Internet cuando reemplazaron a las operadoras por centrales automáticas comenzaron a utilizar sonidos de alta frecuencia para establecer las comunicaciones sin esperar que algunas personas vieran la forma de simular estas frecuencias con algunos adminículos como ocurrió con el silbato del Capitán Crunch.

El uso del silbato del Capitán Crunch o el *Blue box* para "defraudar" a la compañía telefónica son conductas paradigmáticas. Antes de estos dispositivos, un delincuente para defraudar o sustraer bienes de una persona o empresa tenía que tener un contacto personal o ingresar a sus instalaciones para poder engañar personalmente a los empleados o apoderarse personalmente de los bienes; sin embargo, por primera vez la tecnología permitió que el delincuente, amparado en el anonimato y a la distancia, introducirse a la central, por la línea telefónica, y obtener llamadas de larga distancia gratis.

En la era informática los neo delincuentes ya no ingresan o utilizan las redes informáticas para conseguir llamadas telefonicas gratis sino que, protegidos por el anonimato y a la distancia, invaden la privacidad, obtienen información o sustraen fondos. Recientemente una enorme operación criminal a nivel mundial sustrajo 45 millones de dólares en dos bancos de Medio Oriente y los retiró en cajeros

automáticos de 27 países[16]. Este espectacular robo define la actuación de la nueva criminalidad que enfrentaremos en el siglo XXI quienes, en palabras de Loretta Lynch, Fiscal Federal de Brooklyn, "en lugar de utilizar armas y máscaras, esta organización utilizó computadoras e internet."

2.4. La criminalidad informática o la cyber criminalidad.

De acuerdo a Ulrich Sieber[17], el principal estudioso de este tema, la denominación de "computer crime" apareció inicialmente en los periódicos y en la literatura científica en los años 60´s. Un par de décadas más tarde, en la reunión de la OECD[18] en l983 se aceptó la definición de "*computer crime*" o "*computer related crime*" (criminalidad informática o criminalidad relacionada con computadoras) para identificar las conductas ilegales, antiéticas o no autorizadas que involucran procesamiento automático de datos y/o transmisión de datos.

Desde el incio, se evidenció que las nuevas tecnologías sirven como un medio sumamente eficaz para afectar, ya sea como medio para cometer delitos tipificados o cometiendo nuevas conductas que reciben la atención del derecho penal[19]. El derecho tuvo problemas iniciales para afrontar todas las conductas cometidas con el uso de medios informáticos. Los códigos penales fueron elaborados desde la perspectiva de tutelar bienes jurídicos o elementos materiales y no los que se producen a través de ese ciberespacio.

---

[16] La República. Edición del 11.05.13.
[17] Cfr. Sieber, Ulrich. *IUS Informationis. The Internacional Emergence of Criminal Information Law.* Carl Heymans Verlag, Koln. p. 3 y ss.
[18] Organización para la Cooperación y el Desarrollo Económico.
[19] La informática constituye hoy en día una eficiente vehículo para facilitar cualquier conducta criminal En Lima se ha detectado una nueve modalidad empleada para cometer delitos contra el patrimonio. Los delincuentes atraen a sus víctimas con una supuesta "relación amorosa virtual" para luego citarlos supuestamente para conocerse personalmente sin embargo, al llegar a la cita el cyber enamorado es asaltado. Cfr. diario *Correo*, Lima, 19 de febrero de 2005, p. 10.

Y es que se debe considerar que durante la elaboración de los principales códigos penales del siglo XX no era posible prever la existencia de un mundo virtual o la aparición de elementos inmateriales con contenido patrimonial o que se pueda conservar información importante sobre la intimidad o la seguridad nacional o empresarial en medios digitales.

Las conductas desplegadas por la nueva criminalidad que utiliza los elementos tecnológicos colisionaron con el principio de legalidad para tipificar las conductas que aparecían aprovechando las ventajas que ofrecían los avances tecnológicos[20]. De ahí que surge la necesidad de crear tipos penales lo suficientemente flexibles para cubrir las posibles conductas que vulneren los bienes jurídicos tutelados y se dispusieron a preparar una legislación apropiada para enfrentar los retos del uso ilícito de la tecnología.

Así, Günther Kaiser,[21] describe la criminalidad informática como "un fenómeno sometido constantemente a cambios a través del desarrollo técnico y social", en cuyo ámbito nuclear se encuentran "manipulaciones a las computadoras" con el objetivo de conseguir una ventaja patrimonial a favor del autor o de un tercero.

La criminalidad informática al ser practicada por personas hábiles en el manejo de sistemas computarizados creó inicialmente una imagen idílica del hacker o intruso informático que intercede o accede indebidamente un sistema automatizado por una afán lúdico o simplemente para probar su destreza. Sin embargo, la realidad ha demostrado que estas conductas resultan nocivas, ponen en peligro la información almacenada en medios electrónicos y la experiencia ha demostrado que los intrusos pueden causar mucho daño. Uno de los intrusos más famosos,

[20] En una rápida revisión se tuvo claro que no se podía equiparar el concepto de cosa mueble al dinero virtual o las transferencias electrónicas de fondos en los delitos patrimoniales o el concepto de correspondencia al correo electrónico.
[21] Citado por Tiedemann, Klaus; *Derecho Penal y nuevas formas de criminalidad,* Traductor Manuel Abanto, IDEMSA, Lima 2000, p.85.

Kevin Mitnick, conocido por en el mundo hacker como "Condor"[22], fue condenado por acceder a la computadora personal de un especialista en seguridad informática. En 1995 llegó a un acuerdo de culpabilidad[23] aceptando ser culpable de "posesión no autorizada de artefactos de acceso" para recibir una sentencia de 8 meses de prisión.

Los intrusos suelen acceder a sistemas informatizados a través de programas espías o "*troyanos*"[24] que le permite el acceso a distancia del ordenador y poder capturar toda la información que se procesa o almacena. A partir del control del ordenador ajeno[25] el intruso se encuentra en capacidad de obtener los claves secretos de las tarjetas de crédito, de cuentas bancarias, copiar la información o borrar la data. En España se condenó a dos años de pena de cárcel al creador del virus "Cabronator"[26] que afectó cerca de 100.000 usuarios, de los cuales el condenado pudo acceder a sus datos personales de sus discos duros una vez los usuarios visitaban la página que había creado y que instalaba dicho software.

Un gran número de actividades ilícitas en la red están vinculadas a los delitos patrimoniales. A través de la informática se han efectuado estafas aprovechándose de la masiva difusión de las ofertas o subastas en internet[27]. Aunque estas conductas no se encuadran en el tipo penal de estafa han recibido la denominación genérica "fraudes" debido a que esta actividad tiene al engaño como eje central para procurarse un beneficio económico. A través de una página que ofrece

[22] Cfr. *Crime on the internet. 1994-1999*. Jones International and Jones Digital Century.
[23] Plea bargaining.
[24] Se refiere a un virus, programas espías (keylggers o troyanos), softwares que se envían adjunto a un e-mail instalan en la computadora del usuario cuando éste abre el correo; el programa espía captura toda la información que se procesa en la máquina y se reporta al delincuente
[25] La Guardia Civil de Sevilla, en la operación "Canoso" ha detenido al ucraniano L.O., acusado de haber realizado transferencias de dinero a través de Internet de empresas españolas a cuentas de los estafadores. http://www.delitosinformaticos.com/noticias/110613169169580.shtml. En Madrid, en la operación "Tic tac", se detuvo a un programador que introdujo un sofisticado troyano que eludía los programas antivirus y que le permitía el control absoluto de los ordenadores ajenos.
http://www.delitosinformaticos.com/noticias/110598011234424.shtml
[26] Vide Delitosinformáticos.com/noticias/108867367327302.shtml
[27] Quejas en internet subastas…

subastas se ofrecen un producto en subasta para que el público haga su oferta y se escoja la postura más alta; sin embargo, a pesar de pagar el usuario nunca recibe el producto[28].

Los delincuentes informáticos han lanzado una nueva modalidad fraudulenta por la red que no se encuentran en los tipos penales clásicos de estafa o en el reformado artículo 207 del Código Penal español a través del *Phishing* y del desvío de líneas telefónicas a través del Código 806.

Los neodelincuentes utilizan también la tecnología para crear facturaciones fraudulentas en el servicio telefónico. Los delincuentes, a través de diversos medios engañosos consiguen que se marque un número telefónico que contiene el código 806. El código 806 es el número de tarificación adicional[29] que crea una elevada cuenta telefónica.

Un buen ejemplo del uso de la tecnología para facilitar la comisión de delitos ya tipificados se encuentra en los delitos contra la libertad sexual y similares (a la intimidad, por ejemplo). El anonimato en la red favorece la visita de pedófilos para acceder a páginas web con contenido pornográfico o para entablar contacto con menores a través del chat o la transmisión electrónica[30]. En este punto se han reformado las legislaciones para incluir esta conducta a través de la red[31].

---

[28] Cole Bartirorno, de 19 años de edad, ha sido sentenciado por el tribunal federal en California a cumplir una pena de 33 meses de prisión y pagar una multa de 20.000 dólares de indemnización por ofrecer productos en eBay cobrar sus ventas y no remitir los productos vendidos a los compradores. Delitosinformáticos.com/noticias/10746521140417.shtml.

[29] En Alicante se detuvo a 3 personas que obtuvieron 150,000 euros con la modalidad de la verificación adicional. Las víctimas recibían una llamada que les avisaba de que en Correos había un paquete para ellos y que tenían que ponerse en contacto a través de un teléfono, que enmascaraba el 806, y una vez que llamaban procuraban alargar la llamada el máximo tiempo posible. Cfr. delitosinformáticos.com/noticias.

[30] Más de 4.000.000 de sitios en la Red permiten acceder a pornografía infantil de los cuales más de la mitad son de pago. Cada día se crean cerca de 500. El comercio de material pornográfico infantil mueve al año miles de millones de dólares. Se calcula que la explotación sexual comercial infantil afecta a 100 millones de niños y niñas en todo el mundo, víctimas de la prostitución, del turismo sexual, de la trata, tráfico y de la pornografía. (Fuentes: Ecpat Internacional, Unicef).

[31] Así, el Código Penal peruano lo ha tipificado en el artículo 181-A y siguientes.

Es frecuente, en tal sentido, las operaciones policiales que se efectúan con tal finalidad; pero tal vez, el problema estriba en la existencia de un mercado que favorece su compra. Del mismo modo, el hecho que los bancos se nieguen a difundir o siquiera a denunciar los hechos de esta naturaleza por temor a la pérdida de credibilidad de sus operaciones por tarjeta electrónica, lo cual dificulta también la represión de estas conductas ilícitas.

Las primeras manifestaciones de la criminalidad informática[32] eran las manipulaciones o daños en computadoras, espionaje o uso indebido de los sistemas informáticos. En la década de los setentas se realizaron fraudes en seguros que ocasionaron pérdidas de 1 a 2 billones de dólares; las manipulaciones en la empresa sueca "Volvo" entre otros. Esas conductas iniciales, nos informa Sieber, no eran percibidos como crímenes reales, hasta los años ochentas se constató que a través de la informática se vulneraban diversos intereses como la privacidad, el patrimonio, los derechos de autor y las comunicaciones. Adicionalmente, se evidenció el carácter transnacional de estos crimenes en la sociedad de la información actual lo cual impulsó la suscripción de convenios internacionales para enfrentar estas nuevas manifestaciones de la criminalidad.

Siguiendo a Sieber[33], en su bien documentado IUS Informationis, nos informa la primera etapa de las reformas legales aparece en entre los años setentas y ochentas como reacción a las afectaciones a la intimidad ocasionadas por las nuevas posibilidades de recopilar, almacenar o transmitir información a través de las nuevas tecnologías. En este periodo se dictan leyes de protección de la información para cautelar los derechos de la privacidad de los ciudadanos. Una rápida mirada a su evolución, podemos apreciar:

[32] Cfr. Sieber, *IUS Informationis. The Internacional Emergence of Criminal Information Law*... p. 3 y ss.
[33] Cfr. Sieber, *IUS Informationis. The Internacional Emergence of Criminal Information Law*... p. 11.

70’

- Aparecen los primeros estudios sobre el “computer crime”
- Se descubren los primeros casos millonarios de fraudes informáticos
- Se mantiene, sin embargo, una alta “cifra negra” de la criminalidad informática
- Leyes de protección a la información y la privacidad

80’s

- violaciones a la privacidad
- manipulaciones a cajeros automáticos
- uso no autorizado de las telecomunicaciones
- Leyes de represión a las manipulaciones informáticas que afectan al patrimonio
- Leyes de protección a la propiedad intelectual

90’s

Nace la www (World Wide Web) o la red informática mundial a partir de la unión de los sistemas informaticos con las telecomunicaciones que permite el flujo de información de manera inmediata entre los servidores. Como toda la información y gran parte del comercio se transmiten en la red se puede reunir gran cantidad de datos con los cuales, una vez relacionados entre sí, se puedde trazar el perfil del usuario, segmentar la base de clientes y adaptar la oferta a sus gustos, incrementado, así, los beneficios de la empresa la técnica del *spaming* suele llevar aparejada, como ilícita antesala, el seguimiento de los patrones de conducta en la red que permite crear perfiles sobre hábitos de consumo para utilizarlo en el marketing.

Esta plataforma facilitan la comisión de las siguientes actividades:

- Fraudes
- Hacking o "intrusismo"
- Virus
- "Worms" "internet-worms"

Para Möhrenschlager[34] la criminalidad informática se puede dividir en tres categorías:

1. La pérdida del control exclusivo o la confidencialidad(accesos ilegales, obtención de información)
2. La pérdida de la integridad de la información (especialmente a través de la modificación del a información)
3. La pérdida de la accesibilidad.

[34] Information Technology Germany Computer Crimes and Other Crimes against Information Technology in Germany. National Report by Dr. Manfred Möhrenschlager. p. 189.

2.5. Conflicto: privacidad informática contra seguridad

La eclosión de la Red suscita un ámbito de tensión cifrado en la necesidad de tutelar la *privacy* del usuario (traducida en un derecho al anonimato) *versus* seguridad pública y seguridad nacional como intereses colectivos. Pero, por encima de este primer ámbito de tensión, se sitúa otro más amplio; la Red nace como nueva autopista de la información bajo la égida de la anomia, por cuanto la ausencia de regulación jurídica y, por tanto, de límites y de control definen Internet. Sin embargo, la evolución de esta autopista de la información con prontitud ha desvelado la necesidad de abordar su estatuto jurídico; la difusión e identificación de contenidos y conductas ilícitas en la Red y el anhelo de convertir ésta en un nuevo mercado virtual sitúan al poder público en la necesidad de desarrollar los mecanismos jurídicos e institucionales que gobiernen Internet.[35]

Qué duda cabe que este debate cobra especial intensidad en el contexto actual, esto es, a raíz de la crisis suscitada por los atentados del 11 de septiembre de 2001. El temor de que las nuevas tecnologías de la información y, en concreto, Internet, puedan ser utilizadas con fines criminales por delincuentes y, en particular, por organizaciones terroristas, junto a la presión de una opinión pública alarmada tras dichos sucesos, ha determinado que, en el conflicto libertad *versus* control, la

[35] Cfr. Morón Lerma, Esther; *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*. Ed. Aranzadi. 2ª. Ed., Navarra - España, 2002, p.17.

balanza se incline a favor de la seguridad y la prevención, como revela el elenco de disposiciones aprobadas en EE.UU. y en Europa. [36]

De acuerdo a Sieber[37], la prevencion de la criminalidad informatica depende en un alto grado de la eficiencia y seguridad de la tecnologia moderna esto debido a que los delincuentes informáticos se aprovechan de las debiles o las inexistentes medidas de seguridad en los sistemas informáticos a pesar que se recomienda por todos los especialistas la implementación de eficientes medidas de seguridad puesto que a nadie se le ocurriría dejar la puerta de su casa abierta, o las llaves del auto colocadas deberían adoptarse en el seno de las empresas, tanto frente a sus propios empleados como frente a terceros que navegan en la red[38]. Hay que tomar conciencia, de una vez por todas, que debemos tanto particulares como empresas mantener un estándar mínimo de seguridad que cautele adecuadamente la información tratada informáticamente.

La falta o las inadecuadas medidas de seguridad que protegan la intangibilidad de los datos tratados, procesados o almacenados informáticamente en todos los procedimientos de entrada, procesamiento o salida facilitan su vulneración o alteración. Sieber[39] considera que la ley debe establecer niveles específicos de medidas de protección como ocurre en Alemania o en el Reino Unido donde se exigen para proteger datos bancarios o el ente regulador de impuestos. Por mi

---

[36] Cfr. Morón Lerma, Esther; *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red…* pp.22-23.
[37] Sieber, Ulrich. *IUS Informationis. The Internacional Emergence of Criminal Information Law…* p. 95.
[38] Cfr Gutiérrez Francés, M. L.: *Fraude informático y estafa,* op. cit., pgs. 82-83; Romeo Casabona, C. M.: *Poder informático y seguridad jurídica*, op. cit., pg. 40 y Sieber, U.: "Criminalidad informática: peligro y prevención", en *Delincuencia informática*, Mir Puig, S. (Comp.). Barcelona, 1992, pp. 34 y ss. Este último autor dedica un capítulo entero al análisis de las medidas de seguridad de los usuarios de ordenadores, en "Documentación para una aproximación al delito informático", en *Delincuencia informática,* op. cit., pp. 83 y ss.
[39] Cfr. Sieber, Ulrich. *IUS Informationis. The Internacional Emergence of Criminal Information Law…* p. 9.

parte, considero que deben implementarse medidas específicas de seguridad en los sistemas que guarden o procesen información bancaria, financiera, de seguridad nacional o de datos personales.

Así pues, desde las repercusiones de ese *derecho penal postmoderno del riesgo –o de la seguridad-* que parece emerger, la resolución jurídica en Internet, conciliando intereses en tensión, se torna aún más difícil. Dicha complejidad hace necesario destinar, en este trabajo, una especial atención y estudio a la determinación de responsabilidad de los agentes de Internet y, en concreto, de los prestadores de servicios, así como al deber de dichos prestadores de disponer de los medios para la individualización de los autores ilícitos en la red, entre los que se hallan el deber de colaboración para evitar que los contenidos ilícitos se sigan divulgando o el deber de retención de datos relativos a las comunicaciones electrónicas. [40] Es tan importante, para cautelar la información tratada, transmitida, procesada o almacenada en una computadora, la instalación de adecuadas medidas de seguridad que en algunos países se sanciona la negligencia por no instalar medidas adecuadas de seguridad[41].

Ahora bien, en el arbitrio de una solución que trate de conciliar todos esos intereses en conflicto, no puede renunciarse a las garantías dimanantes del derecho penal clásico, en el que prima el individuo frente a la sociedad y, por tanto, no pueden aceptarse las propuestas, iniciadas en EE.UU. y asumidas en Europa, que, con clara vocación expansiva, persiguen una suerte de "neointegrismo punitivo", que cercena fundamentales derechos y principios y que consagra, sin ambages, esa

[40] Cfr. Morón Lerma, Esther; *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red…* p.23.
[41] Cfr. Information Technology. Computer Crimes and Othe Crimes against Information Technology in the United Kingdom. United Kingdom Nacional Report by Prof. Dr. Martin Wasik. p. 492.

indeseable tendencia involucionista, que se hallaba en gestación desde hace ya algún tiempo. [42]

Toda innovación tecnológica acarrea problemas sociales y políticos, puesto que comporta una reorganización de las estructuras sociales afectadas por la innovación. Entre el grupo que cree perder poderes que considera intangibles y el grupo que adquiere una influencia imprevista, se desarrolla una lucha, de cuyo resultado depende la aplicación o el rechazo de la innovación. [43]

Las conductas más destructivas perpetradas en Internet son facilitadas por el anonimato o por el uso de identidades falsas que utiliza para evitar la identificación y persecución penal. Por ello, para poder reprimir delitos cometidos con medios informáticos o en la red es necesario dictar medidas que limiten o eliminen el derecho del usuario al anonimato.

Sin duda, en las sociedades postindustriales el desarrollo de la tecnología y su aplicación a todos los ámbitos de la vida se mantiene una constante tensión entre la defensa de los derechos fundamentales, en concreto, el derecho a la intimidad y la necesidad estatal de proteger la seguridad. En especial el desarollo informático facilita nuevas formas de control e intrusión en la vida privada. Los Estados han adquirido mayor capacidad de control informático con los cuales viene ejercien do mayor control sobre los individuos como las medidas adoptadas por EE.UU, a partir del 11-S, para combatir el terrorismo han supuesto un recorte de garantías y, en algunos casos, una indiscriminada restricción de derechos como cuando se

[42] Cfr. Morón Lerma, Esther; *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red…* p.23.
[43] Cfr. Morón Lerma, Esther; *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red…* p.27.

efectua un mayor control de las comunicaciones electrónicas con programas que identifican palabras claves en los mensajes que puedan ser indicios de actividad criminal.

En este punto hay que tener presente que Sieber[44] nos advierte que la prevención de la criminalidad informática depende en un alto grado de la eficiencia y seguridad de la tecnología moderna debido a que la sociedad post industrial de información requiere de un cambio de paradigma de los bienes corporales o tangibles a los bienes intangibles. El surgimiento de las leyes penales sobre la información requiere de nuevas previsiones legales para la información en general y específicamente para la información almacenada en computadoras.

Por otro lado, el avance de las tecnologías de información y la penetración del internet en todos los ámbitos de la vida han ocasionado que enormes cantidades de información de todo tipo se encuentra tratado o almacenado en sistemas informático sin las debidas medidas de protección. Ante esto surgió la ISO 17799 que propone mecanismos de control para garantizar la seguridad de la información informáticamente tratada o almacenada.

La ISO 17799 sugiere proteger apropiadamente la información la cual considera un activo importante con valor para la organización. De acuerdo a esta norma, se debe implantar o mejorar la seguridad de las bases de datos que protegan de manera adecuada a la información. La seguridad de la información tiene tres grandes ejes:

- **Conservación de confidencialidad** que permite que únicamente accedan las personas autorizadas.

[44] Cfr. Sieber, Ulrich. *IUS Informationis. The Internacional Emergence of Criminal Information Law*… p. 95.

- **Integridad de la información** que mantiene la intangibilidad de la información.

- **Disponibilidad de la información** que permite a las personas autorizadas puedan acceder a ella cuando lo requieran.

2.6. El incontenible avance de la criminalidad en la red. Algunas cifras.

"*La criminalidad por computadoras se incrementa porque ahí esta el dinero*[45]".

Nuestro país, actualmente, se ubica en el sexto lugar en América Latina con mayor actividad maliciosa (ataques cibernéticos) en Internet, según el *Internet Security Threat Report 2011 Trends*[46] sobre amenazas a la seguridad en Internet elaborado por la Corporación Symantec que desarrolla y comercializa softyware en seguridad informática. Los primeros lugares los ocupan Brasil y Argentina.

El informe indica que la cantidad de ataques de hackers en América Latina se elevó un 81% el 2011, lo que representa 5,500 millones de ataques, En el caso del correo electrónico, uno de cada 239 mensajes enviados en la región contiene virus, y los ataques de hackers a celulares casi se duplicaron del 2010 al 2011. En el informe sobre seguridad en la internet preveé para el 2012 que se incrementarán y se especializaran los ataques informáticos, se enviarán malawares más nocivos y

[45] Cfr. Information Technology. Computer Crime and Other Crimes against Information Technology in The United States. National Report by Prof. Edward Wise. p. 511.
[46] Cfr. Internet Security Threat Report . 2011 Trends Volumen 17. Published April 2012. Symantec. www.symantec.com

spams a los destinatarios en internet. Los smartphones y tabletas serán objeto de ataques de malawares.

Finalmente el informe presenta una guía de buenas prácticas en el uso de los sistemas informáticos que contempla que la instalación de antivirus no es suficiente y se debe instalar fuertes estrategias de defensa del sistema informático; encriptar la información sensible Finanlmente, bajo el lema paradigmático *"think before you click"* nos recomienda estar alertas y cautelosos, incluso de los remitentes, que consideramos confiables y seguros. Las descargas de internet solo deben efectuarse desde sitos seguros y no autorizar descargas desde cualquier mensaje o aviso.

El semanario sensacionalista inglés "*News of the world*", integrante del Grupo News Internacional, tuvo que cerrar a raíz del escandalo por revelarse las escuchas ilegales a la Royal British Legion una institución de ayuda económica a soldados heridos o a los familiares de militares fallecidos. En el Perú, el periodista Rudy Palma del diario "Perú 21" se le imputó los cargos de delitos informáticos, violación de las comunicaciones y revelación de secretos de estado por haber accedido ilegalmente a las cuentas de los funcionarios públicos del Ministerio de Comercio Exterior y de congresistas. La defensa de Palma, difundida por los medios, sostiene que él no hackeo los correos (en sentido estricto) sino que éste se habría aprovechado el descuido de los funcionarios que no cambiaron su clave asignada que usualmente es el apellido. Sin embargo, la acción que reconoce el periodista es un acceso indebido o sin autorización de cuentas ajenas.

Como podemos apreciar, el ingreso en la era digital es ya un hecho. Sin embargo, no se nos antojan con una evidencia similar las implicaciones jurídicas que empiezan a desvelarse como consecuencia de la penetración de las nuevas

tecnologías en el tejido socioeconómico. Como ha sido ya observado, los problemas jurídicos que la informática y la telemática someten la sagacidad del jurista dependen de factores en continuo devenir, que convierten el cometido de proporcionar un cuadro normativo coherente en una tarea ardua, si no, en ocasiones, indomeñable. [47]

En el año 2012[48] se denunciaron en el Perú 243 casos en la Fiscalía aunque se estima, basados en los informes de Norton, que debe haber un aproximados de 500,000 agraviados que generan pérdidas aproximadas de US $ 5 millones.

Como podemos apreciar, el ingreso en la era digital es ya un hecho. Sin embargo, no se nos antojan con una evidencia similar las implicaciones jurídicas que empiezan a desvelarse como consecuencia de la penetración de las nuevas tecnologías en el tejido socioeconómico. Como ha sido ya observado, los problemas jurídicos que la informática y la telemática someten la sagacidad del jurista dependen de factores en continuo devenir, que convierten el cometido de proporcionar un cuadro normativo coherente en una tarea ardua, si no, en ocasiones, indomeñable. [49]

En el año 2012[50] se denunciaron en el Perú 243 casos en la Fiscalía aunque se estima, basados en los informes de Norton, que debe haber un aproximados de 500,000 agraviados que generan pérdidas aproximadas de US $ 5 millones.

[47] Cfr. Morón Lerma, Esther; *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Editorial Aranzadi SA, España 2000, p.22.
[48] Cfr. *El Comercio*, Falta de leyes convierte al Perú en paraíso del cibercrimen. edición del 19.12.12.
[49] Cfr. Morón Lerma, Esther; *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Editorial Aranzadi SA, España 2000, p.22.
[50] El Comercio, Falta de leyes convierte al Perú en paraíso del cibercrimen. edición del 19.12.12.

2.7. Principales conductas relacionadas con el uso de la informática y la tecnología de la comunicación mediante las cuales se accede a la computadora, base de datos o se obtiene los datos de información bancaria o financiera.

Es de notar que estas conductas no constituyen un ilícito en sí ni necesariamente lesionan un bien jurídico tutelado en la norma penal sino que pueden ser actos preparatorios de otras conductas delicitvas como obtener la información personal, bancaria o financiera con la cual pueden efectuar transferencias no autorizadas de fondos. Sin embargo, deben ser tipificados por poner en peligro algunos bienes jurídicos.

En efecto, mediante el *phising*, *vishing* o el *pharming* se obtiene los datos de la cuenta bancaria y la clave secreta; empero, con esta acción no se consigue el beneficio económico sino que posteriormente esta información le servirá para efectuar la conducta prevista en el artículo 186 inciso 3, hurto telemático, al acceder a la cuenta de la víctima y transferir sus fondos a cuentas de terceros.

2.7.1. El intruso o hacker.

Bajo la denominación "pirata informático" o "*hacker*" se denominan diversas conductas de puro intrusismo informático en el cual únicamente acceden al sistema pero no alteran los archivos o la información; vulneración de derechos de autor (*craking*) y las de daños informáticos (*ciberpunks* o *ciberpunking*). Se refiere a la introducción de un sistema informático mediante la vulneración de passwords[51].

Durante un tiempo se cuestionaba la necesidad de sancionar el acceso indebido o ilegal pues se consideraba que el hacker o intruso no lesionaba o causaba perjuicio en el sistema diferenciando, incluso esta conducta del cracker o aquel que ingresaba a alterar, destruir datos o programas.

Sobre el tema, Gutierrez Frances[52] sustenta la necesidad de tipificar esta conducta por las siguientes razones: i) los comportamientos de mero intrusismo informático no sancionados se convirtieron en conductas más graves, ii) su tipificación evita la impunidad de otras conductas, iii) sirve como prevención general, iv) ofrece una protección penal autónoma y v) son conductas peligrosas y difíciles de probar cuando poseen dimensión transfronteriza.

La conducta del hacker o el intruso, en la legislación nacional, es una conducta previa y necesaria para la comisión de otras conductas tipificadas[53]. Sin embargo, como veremos más adelante el tipo penal incluye elementos subjetivos de intención trascendente que dificulta su correcta y oportuna represión.

---

[51] Cfr. Mazuelos, Julio. Delitos Informáticos: Una aproximación a la regulación del CP Peruano. En: Revista *Peruana de Doctrina y Jurisprudencia Penales*, Nº 02, año 2001, p. 289.
[52] Cfr. Gutierrez Frances, Maria Luz. *Notas sobre la delincuencia informática: Atentado contra la "información" como valor económico de la Empresa*. En Derecho Penal Económico y de la Empresa. p. 418.
[53] Cfr. Mazuelos, Julio. Delitos Informáticos: Una aproximación a la regulación del CP Peruano. En: Revista *Peruana de Doctrina y Jurisprudencia Penales*, Nº 02, año 2001, p. 289.

2.7.2. Phishing.

La terminología de esta conducta, derivado del verbo *fishing* (pescar), se refiere al envío de e-mail utilizando el nombre de un banco en el cual se coloca un link y web falsa mediante el cual induce al usuario a dar información confidencial sobre sus cuentas bancarias, tarjeta de crédito o su clave secreta. Bajo esta modalidad, muy difundida en nuestro medio, se encuentra la creación de una página web falsa de una institución bancaria para hacer creer a los clientes que se trata de una operación bancaria segura con su banco. En el Perú, los delincuentes envían una falsa página de una entidad bancaria solicitando una actualización de los datos de los clientes; una vez que el usuario actualiza sus datos y sus claves los delincuentes están en capacidad de vaciar todos sus fondos y transferirlas a cuentas de los cómplices.

Esta conducta es precursora de delitos especialmente los patrimoniales ya que permite obtener el login y password de una cuenta bancaria, tarjetas de crédito o sus datos personales con los cuales puede obtener el manejo de las las cuentas obteniendo transferencias no autorizadas o suplantar la identidad ante las entidades bancarias para conseguir créditos a su favor.

2.7.3. **Spaming o publicidad no consentida**.

La conducta de *spaming* consiste en el envío no solicitado de mensajes por correo electrónico a una multitud de desconocidos, ofertando la publicidad de un producto o de un servicio por razones puramente comerciales. Con esta práctica, cualquier buzón de correo electrónico puede ser saturado de mensajes comerciales no deseados e, incluso, un sistema informático entero puede verse bloqueado, si se

ejecuta un programa para que se le envíen mensajes repetidos en cortos espacios de tiempo.

En el ámbito jurídico, esta proliferación del *spam* ha determinado la regulación específica del envío de publicidad masiva no solicitada en la red. En nuestro país se ha regulado el envio de los correos comerciales mediante la Ley Nº 28493 regula el envio de correos electrónicos con fines publicitarios y sanciona con el 1 % de UIT a los spam.

2.7.4. **Clonación de tarjetas. *Skimming*.**

En primer lugar, el delincuente copia con la ayuda de un pequeño dispositivo (*skimmer*) la información de la banda magnética y posteriormente elaboran otra tarjeta con la información para acceder a las cuentas y apoderarse del dinero. Esta modalidad es realizada en establecimientos comerciales con la ayuda de los trabajadores, mozos o cajeros, quienes realizan la copia de la información de la banda magnética.

En primer lugar los delincuentes deben obtener la información financiera de las víctimas que se encuentra grabada en las bandas magnéticas de las tarjetas con la cooperación de los empleados de los establecimientos comerciales quienes aprovechan cuando el cliente entrega la tarjeta para pagar el consumo y utilizan unos pequeños lectores que copian toda la información. Posteriormente, entregan la información a quienes la emplean para clonar el plástico colocando la banda magnetica y los datos de la víctima en ella

2.7.5. Robo de identidad - *identity theft*.

La usurpación de la identidad, es la suplantación de los elementos que identifican a una persona. Esta usurpación de la identidad puede ser parte del engaño de la estafa clásica o como una forma de obtener transferencias electrónicas no

consentidas. Esta modalidad ocasiona enormes perjuicios económicos a los usuarios de los servicios financieros ya que el delincuente efectua transferencias de dinero, compra bienes o servicios, abre o cierra cuentas bancarias o recibe créditos a nombre de aquel. Las suplantaciones de identidad a través de la internet se incrementan de manera alarmante facilitados por la falta de controles de seguridad en los usuarios y alentados por la inadecuada tipificación en los ordenamientos jurídicos.

Usualmente, la víctima recién conoce que le han robado la identidad cuando es reportado como deudor o cuando recibe los avisos de cobranza de las entidades financieras

2.7.6. El vishing.

Mediante esta modalidad los delincuentes envian correos electrónicos con mensajes en los cuales comunican al usuario que se ha cargado una suma alta por consumo telefónico y le indican que si tienen algún reclamo se comuniquen con determinado número telefónico. Cuando la víctima llama le responde una contestadora telefónica de un supuesto banco mediante la cual se le induce a introducir el número de cuenta bancaria y su clave. Con estos datos los delincuentes acceden a su cuenta y pueden disponer del dinero.

2.7.7 El "cambiazo" de tarjetas.

Se trata un método nada tecnológico en el cual el delincuente cuenta con su habilidad y rapidez de predigitador para distraer al usuario de un cajero automático y rápidamente cambiar la tarjeta y entregarle otra inservible. Luego el

delincuente observa la clave secreta del usuario y posteriormente la emplea para acceder a la cuenta bancaria**.**

2.7.8 Los ataques masivos DDoS. La actuación de "Anonymous".

Anonymous es un colectivo que, desde 2008, aglutina a diversos movimientos de hackers que afirman defender la libertad en Internet[54] y se manifiesta en contra servicios públicos, empresas transnacionales y sociedades de derecho de autor realiza acciones en Internet e incluso cuenta con Facebook.

Este grupo se especializan en ataques DDoS o denominados "denegación de servicio" mediante el cual se saturan el ancho de banda para evitar que los usuarios puedan acceder a una página web a una variedad de objetivos que van desde páginas gubernamentales, empresas de servicios, hasta organizaciones de narcotráfico en Mexico. En el Perú esta organización colocó su distintiva careta sobre las páginas web de instituciones estatales e incluso a un partido político revelando datos de sus afiliados.

Los ataques DDoS o de denegación de servicio, (*Denial of Service*) bloquea el acceso a un sistema informático o red por la sature del ancho de banda o sobrecarga su capacidad de procesar las solicitudes de acceso. De esta forma se sobrecarga la red con el envío masivo de solicitudes de acceso ocasionando que el servidor no pueda funcionar normalmente.

[54] http://www.anonops.net

2.7.9 Fraudes mediante llamadas telefónicas.

Los usuarios del sitio sexygirls.com descargaron un visor de imágenes que escondía un troyano que desconcetaba el modem del proveedor del usuario y lo conectaba a un teléfono en Moldavia (URSS) desde donde se redirigía la llamada a los Estados Unidos de Norteamérica. La factura telefónica era astronómica. Este fraude también se realiza con otras páginas web especialmente las de contenido pornográfico.

2.7.10 Los programas dañinos o maliciosos en la red. Malaware.

Se refiere a programas diseñados con el propósito de instalarse en un sistema informático o computadoras con el objeto de obtener información o causar daños. Los últimos virus se han diseñado para controlara el computador y utilizarlas para lanzar ataques DDoS, alojar pornografía infantil o enviar spam. Entre los principales malaware se encuentran:

2.7.10.1. Programas espías. Spyware.

Programas conocidos como *(spyware), webs bugs,* identificadores ocultos y otros dispositivos similares, que pueden introducirse subrepticiamente en el terminal del usuario para acceder a información personal o financiera, archivar datos oculta o rastrear sus actividades. Los *cookies* son subrutinas informáticas o archivos emitidos por un servidor de información y que se almacenan en el disco duro del ordenador visitante. Cuando el usuario acude de nuevo a ese sitio *web*, los datos son reenviados al servidor proporcionándole información actualizada sobre el visitante. Posteriormente los datos se comercializan a empresas dedicadas a ventas por internet o por teléfono.

2.7.10.2. Keyloger

Es un programa que permite registrar todo lo que un usuario ha digitado o tecleado en su computadora y de esta manera obtiene la información personal o bancaria de la víctima.

2.7.10.3. Defacing

Se refiere a la conducta de modificar o alterar no autorizada de una página web. De esta manera se cambia la presentación del sitio web y colocando en su lugar algún mensaje o presentación distinta a la original. Los objetivos de estas acciones son, usualmente, webs gubarnamentales, de agrupaciones políticas o religiosas.

2.7.10.4. Pharming

Consiste en modificar la ruta para acceder a un dominio para desviar al usuario a una página falsa de una de entidades bancarias o para enviar troyanos. De esta forma se obtiene información personal (claves de acceso, número de cuenta).

2.7.10.5. Virus troyano

El virus es un programa que se envía mediante correos electrónicos o en las descargas de Internet (fotos, videos etc). El virus se instala en la computadora y redirecciona al usuario a webs falsas.

El troyano una vez instalado en la computadora envía información a los delincuentes sobre las claves de acceso de la vìctima.

Una manera de introducir el troyano es mediante un correo supuestamente enviado por DHL[55] en el cual se informa que debe recoger un paquete para lo cual se solicita que abra un archivo adjunto que dice contener el formulario para

[55] Cfr. Huerta Casaverde, Henry. *La estafa y otras defraudaciones*. Hala editores, Lima, 2012, p. 254.

recoger el envío de las oficinas. Sin embargo, al abrir el adjunto se descarga el virus mediante el cual se sustraerá información personal del usuario.

2.7.10.6. Gusanos.

Son programas que se difunden en la red ocasionando daños en los datos almacenados en las computadoras.

3. SOBRE EL DELITO INFORMÁTICO.

"*Las nueva tecnologías crean nuevas formas de criminalidad*[56]"

El uso de medios tecnológicos, especialmente las herramientas informáticas, afectan bienes jurídicos tutelados en la legislación actual aunque, en muchos casos, la conducta no puede subsumirse en el tipo penal por exigencia del principio de legalidad.

Los códigos penales clásicos inspirados en los modelos decimonónicos se encuentran estructurados para proteger, básicamente, objetos palpables y visibles. Sieber[57], el principal estudioso de la criminalidad informática, nos informa que en la sociedad post industrial estamos ante el cambio de paradigma del la protección de objetos corporales a la protección de los objetos incorpóreos los cuales, aunque

[56] Information Technology. Computer Crime and Other Crimes against Information Technology in The United States. National Report by Prof. Edward M. Wise. p. 509.
[57] Cfr. Sieber, Ulrich. *IUS Informationis. The Internacional Emergence of Criminal Information Law*… p. 11.

han tenido una incipiente protección a partir de la mitad del siglo XX, han adquirido enorme valor de la información para la economía, cultura y politicas.

En primer lugar, hay que tener claro que la informática ha demostrado ser un importante medio para cometer diversas conductas que afecta intereses jurídicos facilitando o perfeccionando el modo de ejecución de la conducta delictiva. En rigor, no todo delito cometido con el uso de medios informáticos puede denominarse en sentido estricto delito informático ya que en la mayoría de los casos, la tecnología, en general, o la informática, en particular, resulta simplemente un instrumento más para realizar diversos actos excepto en el caso del intrusismo informático "hacking" pues no efectúa ningún daño ni altera la información sólo se infiltra[58]

De acuerdo al Prof. Wise[59] la difusión de las computadoras o más propiamente las tecnologías de la información, que es el resultado de la combinación de las computadoras y las telecomunicaciones, ofrecen una nueva forma de cometer delitos. Para Gutierrez Frances[60] la delincuencia vinculada a las computadoras es más complejo y heterogeneo fenomeno que delitos patrimonial y económico.

El profesor alemán Ulrich Sieber[61] señala que las diferencias que existían entre las legislaciones en lo referido a la a protección de la intimidad o privacidad. En lo concerniente a los delitos económicos por lo general sancionan conductas similares pero existen diferencias en la técnica legislativa en los cuales se puede encontrar dos formas de encarar el problema; por un lado, la ley de delitos informáticos

[58] Cfr. Gutiérrez Frances, Maria Luz. *Notas sobre la delincuencia informática: Atentado contra la "información" como valor económico de la Empresa ...* p.264.
[59] Information Technology. Computer Crime and Other Crimes against Information Technology in The United States. National Report by Prof. Edward Wise. p. 509.
[60] Information Technology. Computer Crime and Other Crimes against Information Technology in Spain. National Report by Dra. María Luz Gutierrez Francés. p. 437.
[61] Cfr. Sieber, Ulrich. *IUS Informationis. The Internacional Emergence of Criminal Information Law*… p. 15 y ss.

chilena contiene una regla general con diversas modalidades como la intrusión, manipulación, destrucción o robo de información y por otro lado, en las leyes norteamericanas y en la mayoría de las legislaciones europeas incorpora a los nuevos objetos y métodos utilizados por el uso de las computadoras ya sea modificando los tipos penales existentes o completando las regulaciones legales.

De a acuerdo a Sieber,[62] La nueva doctrina de "delitos contra el derecho de la información" se desarrolla desde el concepto general de "derecho de la información" y "derecho de la información tecnológica". En concordancia del nuevo concepto de "derecho de la información" reconoce a la información como un tercer factor fundamental aparte de la materia y energía. En un análisis empírico la información comprende los bienes económicos, culturales como un peligro potencial

La nueva teoría del "derecho de la información" resalta el hecho que la tecnología altera las características de la información sin intervención humana a través de procesos automáticos. En un trabajo posterior, Sieber[63] propone desarrollar la nueva doctrina para el "derecho penal de la información" como la respuesta a los desafíos de la sociedad de la información que deberá edificarse sobre la base del concepto "derecho de información y el derecho en la información". En concepto del profesor alemán este nueva rama jurídica se deberá elaborar "en concordancia con las moderna informática e informaciones, el nuevo concepto de "derecho de información" reconoce a la información como el tercer factor fundamental aparte de la materia y la energía".

El profesor Mörhreschlager[64] reconoce la dificultad de identificar adecuadamente las conductas de la criminalidad informatica por lo que afirma "no existe una

[62] Cfr. Sieber, Ulrich. *IUS Informationis. The Internacional Emergence of Criminal Information Law*… p. 15 y ss.
[63] Cfr. Sieber, Uldrich. Ed. IUS Informationis. Information Technology Crime. National Legislations and Internacional Initiatives. Vol. 6. p. 6.
[64] Information Technology. Germany Computer... p. 197.

definicion legal" del delito informático. Luego, citando a Wasik[65] "generalemente, el uso de la computadora in la comision de un delito no altera el hecho que el ilicito haya tenido lugar no cambia la categoria del delito cometido aunque pueda afectar el actual quebrantamiento de la ley y haga mas dificil su deteccion y su procesamiento.

En la doctrina nacional, la profesora García Cantizano[66] entiende que la "delincuencia informática comprende una serie de comportamientos que es difícil reducir o agrupar en una sola definición" debido a que no hay un delito informático sino que sólo es una forma de comisión.

De acuerdo a estas definiciones, puedo afirmar, siguiendo a Gutierrez Francés[67] que se debe emplear el término más exacto, que es "Criminalidad Informática" como una manifestación de la realidad criminal que surge al amparo de las altas tecnologías de la información que afectan a diversas conductas contenidas en el Código Penal.

3.1. El concepto de delito informático.

Unos de los primeros temas a definir son sobre el contenido del "delito informático", pues se trata de un término muy usado para definir conductas en las cuales se constata el uso de la informática o nuevas tecnologías que afectan diversos bienes jurídicos.

Las nuevas tecnologías, especialmente la informática, ha causado un enorme impacto en la vida cotidiana y en el derecho penal. Muchos delitos pueden ejecutarse utilizando estas tecnologías sin afectar el principio de legalidad pero

[65] Information Technology. German Computer Crimes… p. 197 nota 3. Wasik Crime and Computer.
[66] Cfr. García Cantizano, María del Carmen. La delincuencia Informática en el ordeamineto jurídico peruano. En Gaceta jurídica, Tomo 78-B, p. 70.
[67] Cfr. Gutiérrez Frances, Maria Luz. *Notas sobre la delincuencia informática: Atentado contra la "información" como valor económico de la Empresa*… p.261.

también se constata que la informática determina la existencia de nuevas conductas en la cual incluso se afectan nuevos bienes jurídicos.

Reyna Alfaro[68] denomina "delitos computacionales" a todos los delitos que pueden ejecutarse con el uso de medios informáticos mientras que el "delito informático" es aquel que afecta un nuevo bien jurídico; la información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos. No obstante, esta es una definición poco precisa pues casi todos los delitos tipificados en el código penal pueden ser cometidos con el uso de la tecnología o la informática.

De acuerdo a Bramont Arias Torres "No existe una definición aceptada unanimamente sobre lo que es el delito informático pero de modo general es aquel en el que, para su comisión, se emplea un sistema automático de procesamiento de datos[69].

Sin embargo, queda claro que por delito informático se refiere a conductas que utilizan el medio informático para afectar intereses ya protegidos o cuando el uso de la computadora o de los elementos informáticos constituye el objeto de protección.

Como se verá, antes del Código Penal de 1991 las afectaciones del patrimonio individual no se podían sancionar porque los delitos tradicionales que protegían este bien jurídico encontraban una limitación respecto a la cosa mueble como objeto de apropiación.

---

[68] Cfr. Reyna Alfaro, Luis Miguel. Los delitos informáticos. En: *Manual de Derecho Penal Económico*, Lima 2002. p. 323.

[69] Cfr. Bramont Arias Torres, Luis Alberto. El delito informático. En: *Actualidad Jurídica*. p. 71. En el mismo sentido; Mazuelos, Julio. Delitos Informáticos: Una aproximación a la regulación del CP Peruano. En: Revista *Peruana de Doctrina y Jurisprudencia Penales*, Nº 02, año 2001. p. 269. Mazuelos agrega que esto "obedece a la inexistencia de una tipificación específica"

El profesor Nuñez Ponce los considera como "una nueva versión de delitos tradicionales"[70]. Esta afirmación es parcialmente cierta pues, como veremos, un aspecto de la tecnología es servir como un nuevo medio de comisión pero, por otro lado, se constata la aparición de nuevos bienes jurídicos y nuevas conductas propias de la era informática.

La expresión "delito informático" se ha usado de manera coloquial extendiendolo a cualquier conducta en las cuales aparece la informática como medio de comisión o cuando facliita la comisión del delito como en la estafa dofundida por la internet o en la pornografía infantil.

Por mi parte consiero que se puede denominar delito informático cuando una conducta afecte un bien jurídico preciso y concreto que no se encuentre tradicionalmente protegido por el derecho penal. Como es el caso de la seguridad e intangibilidad de los datos almacenados, transmitidos o tratados informáticamente. En este caso, se puede hablar del "delito informático" como un delito autónomo.

De esta manera, la definición de "delito informático" como expresión de la criminalidad informática debe construirse en relación al nuevo bien jurídico merecedor de protección y excluye a las conductas que simplemente utilizan la tecnología o informática como medio para afectar bienes jurídicos diversos ya tutelados en el código.

[70] Nuñez Ponce. *Derecho Informático. Nueva disciplina jurídica para una sociedad moderna*. Ed. Marsol, Lima, p.253.

3.2. Principio de legalidad.

3.2.1. El carácter vinculante de la Constitución.

Hoy nadie discute que la Constitución en sí misma es una norma y, por tanto, exigible por y para todos. Ello es fruto de la evolución del pensamiento humano y de la cada vez mayor importancia y reconocimiento que van adquiriendo los derechos humanos en un Estado social y democrático de derecho, por lo que hoy se concibe a la Constitución no sólo como un amplio espectro de sueños e ideales a alcanzar, sino como verdadera ley suprema que a través de sus normas vincula a todas las personas –naturales o jurídicas- e instituciones de un Estado.

Si, como se ha argumentado, la Constitución peruana es norma jurídica fundamental, la consecuencia necesaria es que todo su contenido es normativo y vinculante. Esto, aplicado de las disposiciones de la Constitución que reconocen los derechos de la persona, significa que los derechos constitucionales vinculan tanto al poder político como a los particulares. Es decir, que los derechos constitucionales son categorías jurídicas plenamente vigentes y que deben ser respetadas por sus destinatarios.[71]

En otras palabras, ninguna ley, persona natural o entidad pública o privada puede sentirse superior o intocable ni ajena a sus disposiciones, ello se basa en la supremacía que nos merece la persona humana, en el respeto a su dignidad[72] y de su libertad que le va a permitir realizar y alcanzar su proyecto de vida. Es de

[71] Cfr. Castillo Córdova, Luis, *Comentarios al Código Procesal Constitucional,* Universidad de Piura, ARA Editores, 1ª. Edición, Lima octubre de 2004, pág. 43. En tal sentido, no le falta razón al profesor Santa Cruz, Julio, en sus *Notas sobre Interpretación y Dogmática en la aplicación de la ley penal,* Revista 4 de la Academia de la Magistratura, Lima 2000, cuando afirma que ..."en el Estado constitucional la ley carece de autonomía porque siempre habrá de rendir cuenta ante la instancia superior de la Constitución."

[72] Fabián Novack y Sandra Namihas. *Derecho Internacional de los Derechos Humanos.* Academia de la Magistratura-GTZ. 1ª. Edición, Lima, noviembre 2004, p.16, sostienen: ..."cuando nos preguntamos dónde radica el fundamento de los derechos humanos (esto es, el por qué) debemos responder que en la dignidad humana, ya que no es posible hablar de ser humano sin dignidad, como tampoco es posible hablar de una vida digna sin libertad, igualdad, integridad, honor (...) el reconocimiento de los derechos humanos es la única manera de garantizarle al individuo una vida digna y, por tanto, su condición de ser humano."

considerar que este respeto a su dignidad se evidencia con mayor intensidad en el Derecho penal, puesto que está en juego la libertad de la persona.

El derecho, a través del aparato normativo, se halla al servicio del hombre coexistencial, para asegurarle el libre desenvolvimiento de su libertad creando situaciones propicias de justicia y seguridad, de todo lo que dinaminará la paz. El hombre, que es un ser libre, requiere, pese a los enormes condicionamientos a que está sometido en su vida, a realizarse según el llamado de su vocación personal, única e intransferible. Para ello exige, necesita poseer los medios adecuados, culturales, económicos, de salud, etc. El derecho, a través de las normas, debe coadyuvar a obtener todo de ello. El derecho es así, debe ser así, liberador. La principal función del derecho es asegurar, mediante la justicia y la seguridad, el que cada hombre, y con él la comunidad toda, se realice y no se frustre.[73]

En tal sentido, los derechos fundamentales representan una importante herramienta para el logro de tales fines. Actualmente, se reconoce que los derechos fundamentales presentan una doble dimensión: subjetiva y objetiva. En su concepción inicial, los derechos fundamentales eran simples límites al ejercicio del poder público, es decir, garantías negativas para tutelar los intereses individuales.

Hoy día se han convertido, además, en un conjunto de valores o fines directivos de la acción positiva del Estado y sus instituciones. Por tanto, los derechos fundamentales responden hoy día a un conjunto de valores y principios de vocación universal, que informan todo el contenido del ordenamiento infraconstitucional. En su dimensión subjetiva, es evidente que los derechos fundamentales determinan el estatuto jurídico de los ciudadanos, al mismo tiempo que enmarcan sus relaciones con el Estado y con los demás particulares. De esta

[73] Cfr. Fernández Sessarego, Carlos; *Libertad, Constitución y Derechos Humanos*, Centro de Investigaciones Judiciales de la Corte Superior de Justicia de Ica, 1ª. Edición. Lima 2003, pp. 14-15.

formas, tales derechos tienden a proteger la libertad, autonomía y seguridad de la persona no sólo frente al poder público, sino también frente a los demás miembros de la comunidad.[74]

De Asís Roig,[75] sostiene que el papel de los derechos fundamentales en una sociedad moderna es claro. Estos derechos constituyen la base de todo sistema político que postule como fin fundamental el desarrollo de la dignidad humana y, por otro lado constituyen las exigencias, necesidades y pretensiones vitales de los hombres. El conocimiento de su significado, de su importancia, de la posibilidad de su ejercicio, es fundamental no solo para toda persona sino también para el porvenir de la humanidad. Podemos así afirmar, con Eusebio Fernández, que la defensa de los derechos humanos fundamentales se presenta como un auténtico reto moral de nuestro tiempo, la piedra de toque de la justicia del Derecho y de la legitimidad del Poder y el procedimiento garantizador de la dignidad humana contra todo tipo de alienación y manipulación.

Sobre el tema, el tribunal español[76], sostuvo que: "Nuestro Tribunal Constitucional se ha referido a la dignidad humana considerándola como un valor espiritual y moral inherente a todas las personas, que se constituye en un *minimum* invulnerable que todo estatuto jurídico debe asegurar, y que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida (esto es en la autonomía individual), constituyendo el punto de arranque para la existencia y especificación de los derechos fundamentales (STC 27/82, 53/85, 57/94). (…) los derechos se configuran como los principales instrumentos para el logro de la dignidad, por lo que esta adquiere sentido desde el examen de los bienes que los derechos protegen."

---

[74] Cfr. Hernández Valle, Rubén; *Derechos fundamentales y Jurisdicción constitucional,* Jurista Editores, 1ª. Edición, Lima marzo 2006, p. 29.
[75] Cfr. De Asís Roig, Rafael; *Escritos sobre Derechos Humanos,* ARA Editores, 1ª. Edición, Lima 2005, p.54
[76] Citado por De Asís Roig, Rafael; *Escritos sobre Derechos Humanos...* pp. 71-72.

Es evidente, entonces, que el artículo 1 de la Constitución que sostiene que la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado, adquiere real valía y se materializa en el momento de la interpretación y aplicación de los derechos fundamentales a cada caso en concreto,[77] en los que se debe considerar como guías de nuestro actuar el principio *pro homine*[78], la fuerza expansiva, irrenunciabilidad, posición preferente y de eficacia que tienen los derechos fundamentales.[79] Sólo de esta manera podemos hacer realidad la efectiva y adecuada protección de la persona y su dignidad, y que dicho artículo constitucional no quede como una fórmula abstracta, inmaterial o simple quimera intelectual.

Este es el criterio asumido por el Tribunal Constitucional peruano; así, por todos y a manera de ejemplo, es de señalar que en el Exp. No. 010–2002–AI/TC - Caso Marcelino Tineo Silva[80], se sostiene que la dignidad de la persona humana es el fundamento de los derechos fundamentales en un estado social y democrático de

---

[77] Como señala Gustavo Zagrebelsky, la …"interpretación jurídica es una actividad eminentemente práctica, en el sentido de que procede de casos prácticos y tiene como finalidad su resolución." Citado por Edgar Carpio Marcos en *La interpretación de los derechos fundamentales,* Ed. Palestra, 1ª. Edición, Lima 2004, p.18.

[78] Cfr. Hernández Valle, Rubén; *Derechos fundamentales y Jurisdicción constitucional*… p.46, afirma que: "El citado principio, junto con el de *pro libertatis,* constituyen el meollo de la doctrina de los derechos humanos y significa que el derecho debe interpretarse y aplicarse siempre de la manera que más favorezca al ser humano."

[79] El Tribunal Constitucional Federal alemán, citado por Edgar Carpio Marcos en *La interpretación de los derechos fundamentales…* p. 30, en el BverfGE, 6, 55 (72) sostuvo que …"incumbe a la jurisprudencia constitucional descubrir la diferente función de una norma constitucional y en particular de un derecho fundamental. Y al respecto se dará preferencia a la interpretación que más fuertemente despliegue la eficacia jurídica de la norma."

[80] Véase también STC Exp. No.03052-2009-AA/TC – Caso Yolanda Lara Garay; STC Exp. No.1317-2008-PHC/TC - Francisco Antonio Gregorio y Juan Felipe Gaspar José Tudela Van Breugel Douglas a favor de Felipe Tudela y Barreda; Exp. N.° 02448-2008-PHC/TC - Javier Sulca Cáceres y otros; Exp. N.° 04723-2008-PHC/TC - Alberto Laucata Suña; Exp. N.° 02068-2008-PHC/TC - Eliseo Chavarria Vilcatoma; Exp. No.1417 – 2005 – AA/TC – Manuel Anicama Hernandez; Exp. No.0044-2004-AI/TC- Congresistas de la República, Exp. No.0042 – 2004- AI/TC – Luis Lobatón Donayre y otros; STC Exp. No.00050-2004-AI/TC – Colegio de Abogados del Cusco y otros; STC Exp. No.02273-05-PHC/TC – Karen Mañuca Quiroz; STC Exp. No.02313-HC/TC – Luz Margarita Bustamante Candiotti; STC Exp. No.02049-AA/TC – Guillermo Gonzales Neumann; STC Exp. No.03179-2004-AA/TC – Apolonia Ccollcca Ponce; STC Exp. No.00537-2007-AA/TC – Rosario López de Zapata; STC Exp. No.0008-2003-AI/TC – Roberto Nesta Brero y otros.

derecho. Textualmente señala: "La dignidad de la persona humana es el presupuesto ontológico para la existencia y defensa de sus derechos fundamentales. El principio genérico de respeto a la dignidad de la persona por el sólo hecho de ser tal, contenido en la Carta Fundamental, es la vocación irrestricta con la que debe identificarse todo Estado Constitucional y Democrático de Derecho. En efecto, este es el imperativo que transita en el primer artículo de nuestra Constitución."

Consecuentemente, de lo expuesto se colige que, en nuestro ordenamiento jurídico, el primer rango normativo –es decir, vinculante- corresponde a la Constitución y el segundo a la ley y a las normas con rango de ley y así sucesivamente. Que el sustento de ese carácter vinculante constitucional lo encontramos en la persona humana y en el respeto de su dignidad.

3.2.2 El principio de legalidad como fundamento de la actividad persecutoria.

En cuanto al principio de legalidad penal, cabe señalar que el artículo 2º. inciso 24, literal "d", de la Constitución Política del Perú, establece que: "Toda persona tiene derecho: (...) 24. A la libertad y a la seguridad personales. En consecuencia: (...) Nadie será procesado ni condenado por acto u omisión que al tiempo de cometerse no esté previamente calificado en la ley, de manera expresa e inequívoca, como infracción punible, ni sancionado con pena no prevista en la ley".

Con tal tenor se consagra el principio de legalidad penal, el que no sólo se configura como principio propiamente dicho, sino también como derecho subjetivo constitucional de todos los ciudadanos. Como principio constitucional informa y limita los márgenes de actuación de los que dispone el Poder Legislativo y el Poder Judicial al momento de determinar cuáles son las conductas prohibidas, así como

sus respectivas sanciones. En tanto que, en su dimensión de derecho subjetivo constitucional, garantiza a toda persona sometida a un proceso o procedimiento sancionatorio que lo prohibido se encuentre previsto en una norma previa, estricta y escrita, y también que la sanción se encuentre contemplada previamente en una norma jurídica.[81]

El principio de legalidad constituye, pues, una auténtica garantía constitucional de los derechos fundamentales de los ciudadanos y un criterio rector en el ejercicio del poder punitivo del Estado Democrático.[82] Esto significa que el principio de legalidad obliga al Estado, por un lado, a preocuparse por disponer de los medios o instrumentos más eficaces para prevenir el delito y, por el otro, a encontrar -dentro del ordenamiento jurídico- limites a su actividad punitiva.[83] De no ser por el principio de legalidad, el ciudadano quedaría en las más completa indefensión o desamparo, ya que, a falta de la ley, reinaría la inseguridad y con ella la arbitrariedad[84], o simplemente la ley del más fuerte.

Por esta razón se sostiene que el Estado no puede intervenir en todos los fueros del ciudadano, en virtud de sus cuatro consecuencias o manifestaciones que representan una barrera infranqueable y que permite, no solamente el respeto de las libertades ciudadanas[85], sino también el mantenimiento incólume de los fundamentos del mismo Estado democrático de Derecho.[86]

---

[81] Cfr. STC Exp. N.° 03987-2010-PHC/TC - Alfredo Alexander Sánchez Miranda; STC Exp. N.° 03245-2010-PHC/TC - Jesús Belisario Esteves Ostolaza; STC Exp. N.° 2758-2004-HC/TC.
[82] Cfr. STC Exp. No.2192-2004-AA/TC – Gonzalo Costa Gómez.
[83] Cfr. Urquizo Olaechea, José; *La Constitución comentada,* Obra colectiva, Ed. Gaceta Jurídica, Lima 2005, p.279.
[84] De su parte, Heinkel, Heinrich; *Introducción a la Filosofía del Derecho*. Traducción de Enrique Gimbernat Ordeig. Madrid, 1968, p. 546, sostiene: "la seguridad jurídica, y por ende la ley, se opone a la incertidumbre, al azar, a la arbitrariedad y al desamparo frente a una situación de regulación".
[85] Cfr. Cavero Lataillade, Iñigo y Zamora Rodríguez, Tomás; *Introducción al Derecho Constitucional*. Editorial Universitas, Madrid, 1996, p. 145.
[86] Sobre los fundamentos o características del Estado democrático de Derecho y su relación con la ley, la seguridad jurídica y las libertades, vide Ramírez Cardona, Alejandro; *El Estado de la Justicia*. (Más allá del Estado de Derecho). Editorial Temis, Bogotá, 1996, pp. 182 y ss.

En un Estado de Derecho se debe salvaguardar el reinado del principio de legalidad. Su vigencia es irrenunciable y su violación injustificable[87], porque esta institución jurídica -desde que fue introducida al Derecho Penal por Feubarch[88] hasta la actualidad- representa la plataforma más sólida de todo el andamiaje de garantías que el ciudadano tiene frente al Estado.

Y es que debe tenerse presente que la vigencia del principio de legalidad es sinónimo de cristalización material del parágrafo 1 de la Carta Jurídico-Política, pues permite la ampliación y desarrollo de los ámbitos de libertad del ciudadano y, por tanto, del desarrollo pleno de sus potencialidades humanas. Por el contrario, la violación, cualquier fisura o relajamiento del principio de legalidad implica el directo e inmediato aniquilamiento de las garantías penales y constitucionales de los ciudadanos, así como de los mismos fundamentos del Estado de Derecho.[89]

---

[87] Cfr. Cobo del Rosal, Manuel y Vives Antón, Tomás; *Comentarios al Código Penal español*. Dirigido por Manuel Coba del Rosal, Madrid 1999, p. 25, afirman que: "El principio de legalidad globalmente considerado, solo puede imaginarse como inatacable, como el enunciado más inexorable de los que articulan el Derecho Penal de un Estado democrático de Derecho que consagra la justicia como valor superior del ordenamiento".

[88] Como lo sostiene Urquizo Olaechea, José; *La Constitución comentada*… p.280, …"si bien es cierto; el penalista germano Feuerbach es quien introduce en el Derecho Penal el principio *Nullum crimen, nulla poena sine lege;* recién a comienzos de! siglo XIX, esta institución jurídica, propia de todo el ordenamiento jurídico romano-germánico, tiene un largo proceso de gestación que comienza con las ideas iluministas que buscaron mayores cuotas de justicia. Con la Filosofía de la Ilustración surgieron los planteamientos del contrato social y la división de poderes, los cuales fueron desarrollados por Rousseau y Montesquieu para debilitar las bases de! *ancian régimé* francés. Asimismo, e! racionalismo iluminístico -que inspiró e! surgimiento de los principios de libertad, igualdad y fraternidad, los mismos que se levantaron contra e! aparato judicial y de ejecución arbitrarios de esa época- ejerció una enorme influencia en los penalistas de entonces (v.gr. Beccaria y Feuerbach) quienes, basados en los ideales del Siglo de las Luces, introdujeron al Derecho Penal el principio *Nullum crimen, nulla poena sine lege;* que solo puede ser dado por el Poder Legislativo."

[89] Cfr. Ferrajoli, Luigi; *El garantismo y la Filosofía del Derecho*. Traducción de Gerardo Pisarello / Alexei Julio Estrada / José Manuel Díaz Martín. Universidad Externado de Colombia, Bogotá, 2000, p. 66. Este autor concibe que el Estado de Derecho se caracteriza por tres principios: "a) el principio de legalidad de toda la actividad del Estado, es decir, de su subordinación a las leyes generales y abstractas emanadas de órganos políticos-representativos y vinculadas a, su vez, al respeto de ciertas garantías fundamentales de libertad; b) el principio de publicidad de los actos, tanto legislativos como administrativos y judiciales; c) la sujeción a control de todas las actividades estatales, bajo la doble forma de control jurisdiccional de legitimidad: ejercido por jueces independientes; y de control político, ejercido por el Parlamento sobre los aparatos ejecutivos y administrativos y por los electores sobre el Parlamento."

Pero también es de mencionar que tal principio contiene y garantiza, a su vez, la prohibición de la aplicación retroactiva de la ley penal (*lex praevia*), la prohibición de la aplicación de otro derecho que no sea el escrito (*lex scripta*), la prohibición de la analogía (lex stricta) y de cláusulas legales indeterminadas (*lex certa*). Sin embargo, el primero de los enunciados, esto es la prohibición de la retroactividad de la ley penal, tiene una excepción con sustento constitucional que es la contenida en el segundo párrafo del artículo 103 de la Constitución que señala "Ninguna ley tiene fuerza ni efecto retroactivo, salvo en materia penal, cuando favorece al reo"...

En otras palabras, en nuestro sistema jurídico, únicamente la ley es la fuente vinculante de jueces, fiscales, políticos y ciudadanos. La jurisprudencia, la costumbre, la doctrina, los principios generales, etc., no vinculan a las personas ni a las instituciones, y por tanto, no pueden ser fuente creadora de derecho.[90]

Cuando Feuerbach originó los fundamentos de la célebre fórmula enunciada en latín "*nullum crimen, nulla poena sine lege*",[91] asentó las bases del principio de legalidad, el cual, ha derivado analíticamente en diversas garantías, las cuales son:

a. ***Garantías sustantivas***. Consiste en que no hay tipo penal, pena y medida de seguridad sin ley escrita, estricta, cierta y previa; al respecto Ferrajioli comenta lo siguiente: "Dos logros fundamentales de la teoría clásica del derecho penal y de la civilización jurídica liberal se traban con esta concepción. El primero es la garantía para los ciudadanos de una esfera

[90] Sobre el tema, compartimos el criterio expuesto por Urquizo Olaechea, José; *La Constitución comentada*… p.281, cuando sostiene que: "Debemos precisar que nosotros no negamos que la jurisprudencia, la costumbre, los principios generales y la doctrina son fuentes del Derecho Penal. Lo que afirmamos es que estas fuentes aludidas no obligan al legislador a crear delitos y penas, al juez a condenar o absolver a una persona y al ciudadano a adecuar su conducta. En el Derecho Penal la jurisprudencia, los principios generales, el derecho consuetudinario y la doctrina, sirven como complemento del desarrollo integrador del Derecho, o sea, como mecanismos que ayudan a precisar conceptos, siempre y cuando no perjudiquen a los ciudadanos. Al respecto véase in extenso Castillo Alva, José Luis. *Principios de Derecho Penal*. Parte General. Gaceta Jurídica, Lima, 2002, p. 24.

[91] Este principio fue incluido en la "Declaración de derechos del hombre y del ciudadano" de 1789 y un poco antes en la declaración norteamericana de Filadelfia de 1774.

intangible de libertad**,** asegurada por el hecho que al ser punible sólo lo que está prohibido por la ley. El segundo es la igualdad jurídica de los ciudadanos ante la ley: las acciones o los hechos, cualquiera que los cometa, pueden realmente ser descritos por las normas como "tipos objetivos" de desviación y, en cuanto tales, ser previstos y probados como presupuestos de iguales tratamientos penales.[92] Esta garantía implica tanto al legislador (como dador de las normas) como a los jueces (como aplicadores de las leyes) una visión de las normas legales dentro de un Estado de Derecho, es decir, que éstas no sólo sean vigentes, sino también, válidas.

b. ***Garantías procesales.*** Consiste en que nadie puede ser castigado sino en virtud de un proceso legal, y que la norma penal sólo puede ser aplicado por los órganos y los jueces instituidos por la ley para esa función *("nemo damnetur nisi per legale iudicium; nemo iudex sine lege")*.

c. ***Garantías de ejecución penal.*** Consiste que no hay pena ni medida de seguridad sin adecuado tratamiento penitenciario y asistencial, sin tratamiento humanitario, y sin resocialización *("nulla poena nulla mensura sine regimene legale, sine humanitae, sine resocializatione")*.

De los tres tipos de garantías, sólo incidiremos en las garantías sustantivas, las cuales, Muñoz Conde comenta de la siguiente forma: …"no cabe calificar de delito a las conductas que no se encuentran definidas como tales por la ley, incluso aunque sean desvaloradas socialmente o consideradas deshonestas o inmorales; del mismo modo, a las conductas delictivas no pueden aplicárseles penas distintas de las que están previstas en la ley".[93] El citado autor desprende una serie de principios a partir de estas garantías, las cuales son: *a*) el principio de reserva de

[92] Cfr. Ferrajoli, Luigi; *Diritto e ragione. Teoría del garantismo penale*. Bari, 1989, p. 36.
[93] Cfr. Muñoz Conde, Francisco / García Arán, Mercedes. *Derecho Penal Parte General*, Madrid, p. 103

ley; *b*) el principio de taxatividad y seguridad jurídica; *c*) el principio de prohibición de retroactividad; *d*) el principio de prohibición de analogía y *e*) el principio *non bis in idem*.

En lo que respecta al principio de taxatividad y seguridad jurídica, éste consiste en que la ley debe establecer la conducta punible en forma clara y concreta; por lo que, se debe evitar el empleo, en los tipos penales, de conceptos excesivamente vagos, los cuales, no posibiliten una interpretación segura (por parte del juez), así como una enumeración excesivamente casuística.[94]

Este principio busca supuestos de hecho claros, así como, una interpretación judicial que no altere el contenido material de la norma jurídico-penal.

En lo que respecta, al principio de prohibición de analogía, éste consiste que, está prohibida la aplicación por analogía de la ley penal (art. 139 inc. 9 Const.)[95]. Por analogía se entiende al proceso por el cual son resueltos los casos no previstos en la ley, extendiéndoles a ellos las disposiciones previstas para casos semejantes. Sin embargo, el art. III del T.P. del C.P. establece la prohibición de la analogía perjudicial o *in malan partem*, al prescribir lo siguiente: "No es permitida la analogía para calificar el hecho como delito o falta, definir un estado de peligrosidad o determinar la pena o medida de seguridad que les corresponde".[96]

---

[94] Cuestión aparte son los tipos abiertos, los cuales, el Juez los debe de cerrar para subsumir la conducta; no obstante un sector de la doctrina peruana precisa que todos los tipos penales de la parte especial son abiertos, porque el Juez debe tener presente las normas penales de la parte general (ej: tentativa, autoría y participación, determinación de la pena, entre otros).

[95] (…) 9. El principio de inaplicabilidad por analogía de la ley penal y de las normas que restrinjan derechos.

[96] Cfr. Villavicencio Terreros, Luís Felipe. *Derecho Penal – Parte General*. Ed. Grijley. Lima 2006, p. 63. "La prohibición de la analogía sólo se aplica a la analogía perjudicial para el inculpado (*analogía in malam partem*), es decir, aquella que extiende los efectos de la punibilidad. Por el contrario, la analogía favorable (*analogía in bonam partem*) es aceptada a través de los procesos de interpretación que extienda analógicamente circunstancias atenuantes o causales personales de exclusión de la punibilidad".

Finalmente, en lo que respecta, al principio "*non bis in idem*", éste consiste en la prohibición de que un mismo hecho resulte sancionado más de una vez.

Empero, es necesario dejar establecido que no debe identificarse el principio de legalidad con el principio de tipicidad. El primero, garantizado por el ya mencionado ordinal "d" del inciso 24) del artículo 2° de la Constitución, se satisface cuando se cumple con la previsión de las infracciones y sanciones en la ley. El segundo, en cambio, constituye la precisa definición de la conducta que la ley considera como falta.

3.2.3 El principio de imputación necesaria y derecho de defensa.

Este principio está implícito en el artículo 8.2.b de la Convención que señala el derecho del inculpado a la comunicación previa y detallada de la acusación formulada. Este derecho es esencial para el ejercicio del derecho de defensa pues el conocimiento de las razones por las cuales se le imputa a alguien la presunta comisión de un delito, permite preparar adecuadamente los argumentos de descargo. Este derecho se ve satisfecho si se indica con claridad y exactitud las normas y los supuestos de hecho en que se basa la acusación.[97]

Recordemos que este principio es inherente al principio acusatorio e implica que la imputación no sólo debe ceñirse a la existencia o no de la comisión de un delito, sino –sobre todo- a que la comisión de tales hechos estén vinculados –a través de pruebas indiciarias- con su presunto autor o autores[98], por lo que la imputación

[97] Cfr. Huerta Guerrero, Luis Alberto. *El debido proceso en las decisiones de la Corte Interamericana de Derechos Humanos.* Comisión Andina de Juristas. Lima, octubre de 2003, p. 51.

[98] Cfr. Vásquez Vásquez, Marlio, en su *¿Cómo enfrentar el mandato de detención?,* publicado en la revista *Actualidad Jurídica No.136,* Ed. Gaceta Jurídica, Lima, marzo 2005, pág. 14, nos dice: "Puede entenderse que en un caso concreto exista suficiencia probatoria sobre la realización de un hecho delictivo, pero resulta totalmente diferente a ello que existan suficientes elementos probatorios respecto a la participación delictiva del procesado en ese hecho concreto. Puede contarse con suficientes elementos probatorios sobre la existencia

(hechos/presunto autor) debe realizarse de manera concreta, cierta e individualizadamente –lo que en doctrina se denomina *nexo causal*- de ningún modo puede generalizarse, pues implicaría una afectación al derecho de defensa[99] y al principio de presunción de inocencia.

Sólo con una clara y precisa imputación de los hechos podremos hablar de que los justiciables en un proceso penal se encuentran de manera efectiva en igualdad de armas[100] y se promoverá adecuadamente el contradictorio, permitiendo a la defensa contradecir no sólo la prueba de cargo, sino también la propia calificación jurídico-penal que se le imputa.[101]

---

de un delito de homicidio, porque conocemos la presencia del cadáver y la causa violenta de la misma, pero no existir suficientes elementos probatorios respecto a la participación del imputado en ese hecho."

[99] Cfr. Tiedemann, Klaus. *Constitución y Derecho Penal.* Palestra Editores. 1ª. Edición, Lima 2003, p. 212, afirma que: "La protección de los Derechos Humanos en el proceso de partes (nosotros también consideramos que aun en el modelo de proceso inquisitivo reformado) empieza y termina con que todo inculpado en todo proceso penal tenga de su parte una defensa eficiente, bien preparada, en *igualdad de armas* con la acusación."

[100] Oña Navarro, en su *El derecho de defensa en la fase de instrucción del proceso penal en la doctrina del Tribunal Constitucional,* En: *Constitución y garantías procesales,* revista del Consejo General del Poder Judicial, Madrid – España 2004, p. 215, cita la STC 178/2001 expedida por el Tribunal Constitucional español, que afirma: "Del principio de igualdad de armas, lógico corolario del principio de contradicción, se deriva asimismo la necesidad de que las partes cuenten con los mismos medios de ataque y defensa e idénticas posibilidades y cargas de alegación, prueba e impugnación, a efectos de evitar desequilibrios entre sus respectivas posiciones procesales, sin que sean admisibles limitaciones a dicho principio, fuera de las modulaciones o excepciones que puedan establecerse en fase de instrucción (o sumarial) por razón de la propia naturaleza de la actividad investigadora que en ella se desarrolla, encaminada a asegurar el éxito de la investigación y, en definitiva, la protección del valor constitucional de la justicia." Por su parte, Pedro Angulo Arana en *La función del fiscal,* Jurista Editores, 1ª. Edición, Lima marzo 2007, p. 181, sostiene que: "Podría argumentarse que considerar parte al Ministerio Público constituye una necesidad para despojarle así de *imperium* y constituirlo en igualdad de condiciones con el procesado o procesados, de modo que concurra con aquellos en igualdad de armas y no exista ventaja a su favor. En realidad como dice Iñaki Esparza, la igualdad de armas se configura de modo distinto en cada realidad, según se configure la acción penal como pública o no. Sin embargo, llega a concluir que los medios que posee el Estado son infinitamente mayores a los que el inculpado podría emplear en su defensa. Esa realidad es reconocida en la doctrina alemana, donde se prefiere hablar de igualdad de oportunidades o "chancengleichheit". En realidad, la igualdad de armas, en tanto igual condición, instrumentos y potestades resulta imposible de conseguir y sólo puede tratarse durante el juicio oral (al tratar) de equilibrar las oportunidades dadas a la defensa con las concedidas a la acusación."

[101] Oña Navarro, *El derecho de defensa en la fase de instrucción del proceso penal en la doctrina del Tribunal Constitucional…* sostiene: "En todo caso, la contradicción ha de extenderse tanto a la oposición o discusión sobre las pruebas aportadas y practicadas sobre los hechos que sirven de soporte a las imputaciones como a las cuestiones procesales y jurídicas (así, la STC 33/2003, del 3 de febrero de 2003, reitera que el derecho de defensa comprende no solo el derecho de alegar y contradecir los hechos objeto de acusación sino también los elementos esenciales de la calificación jurídica, al afirmar "*el derecho de defensa y el derecho a ser informado de la acusación… tiene por objeto los hechos considerados punibles, de modo que sobre ellos*

Así lo ha señalado el Tribunal Constitucional español, en su STC 176/1998:[102] cuando resolvió que ello …"constituye una exigencia ineludible vinculada a un proceso con todas las garantías, para cuya observancia adquiere singular relevancia el deber de los órganos jurisdiccionales de posibilitarlo." Más adelante, en la misma sentencia se lee: "Del principio de igualdad de armas, lógico corolario del principio de contradicción, se deriva asimismo la necesidad de que las partes cuenten con los mismos medios de ataque y defensa e idénticas posibilidades y cargas de alegación, prueba e impugnación, a efectos de evitar desequilibrios entre sus respectivas posiciones procesales, sin que sean admisibles limitaciones a dicho principio, fuera de las modulaciones o excepciones que puedan establecerse en fase de instrucción (o sumarial) por razón de la propia naturaleza de la actividad investigatoria que en ella se desarrolla, encaminada a asegurar el éxito de la investigación y, en definitiva, la protección del valor constitucional de la justicia."[103]

A mayor abundamiento, Tiedemann[104] sostiene que una condición previa absolutamente necesaria para toda defensa es la de conocer el contenido de la imputación en el primer interrogatorio, sea policial o judicial. Omitir esta información al inculpado es lo mismo que tratarle como objeto del proceso, que se desarrolla sin su activa participación y sin contradicción posible. Es solamente con el conocimiento de la imputación cuando el inculpado puede decidir si se defiende de manera activa o guarda silencio.

---

recae precisamente la acusación y sobre ellos versa el juicio contradictorio… pero también la calificación jurídica, dado que ésta no es ajena al debate contradictorio.").

[102] Citado por Jaén Vallejo, Manuel. *Justicia penal contemporánea.* Ed. Portocarrero. 1ª. Edición. Lima, agosto de 2002, p.77.

[103] Citado por Oña Navarro, *El derecho de defensa en la fase de instrucción del proceso penal en la doctrina del Tribunal Constitucional*… , p.214.

[104] Cfr. Tiedemann, Klaus. *Constitución y Derecho Penal*… p.185.

El Tribunal Constitucional peruano, en la reconocida sentencia del Exp. No. 3390-2005-PHC/TC – Caso Margarita Toledo Manrique[105], sostuvo que se viola al principio de imputación necesaria al no precisar, en el auto apertorio, la modalidad delictiva que se le atribuye y que genera estado de indefensión. Igualmente, como afectación al principio de imputación necesaria, en el Exp. No.0056-2004-HC/TC – Caso Manuel Contreras Cardoso[106], el Tribunal Constitucional sostiene que se viola este principio cuando no se precisa el tiempo y las circunstancias en que ocurrieron los hechos.

Tenemos también el Caso Víctor Raúl Martinez Candela, Exp. No.1166-2003-HC/TC, en el que se establece la relación existente entre el principio de imputación necesaria y el derecho de defensa. Así: "[...]Respecto a la supuesta falta de fundamentación en la imputación del delito de prevaricato, el artículo 77° del Código de Procedimientos Penales, modificado por la Ley N.º 24388, establece que el auto apertorio de instrucción "expresará la calificación de modo específico del delito o los delitos que se imputan al denunciado." Dicha disposición legal guarda directa relación con el derecho de defensa, pues sólo conociendo cabalmente la conducta que se le atribuye y la falta que se le imputa, podrá el inculpado ejercer eficazmente los medios de defensa que la ley le franquea. En el presente caso,

[105] En dicha sentencia se dice literalmente: Así: [….] "el juez penal cuando instaura instrucción por el delito por falsificación de documentos en general, omitiendo pronunciarse en cuál de las modalidades delictivas presumiblemente habría incurrido la imputada, y al no precisar si la presunta falsificación de documentos que se imputa a la favorecida está referida a instrumentos públicos o privados, lesiona su derecho a la defensa, toda vez que, al no estar informada con certeza de los cargos imputados, se le restringe la posibilidad de declarar y defenderse sobre hechos concretos, o sobre una modalidad delictiva determinada y, con ello, la posibilidad de aportar pruebas concretas que acrediten la inocencia que aduce. Esta omisión ha generado un estado de indefensión que incidirá en la pena a imponerse y en la condición jurídica de la procesada, lo cual demuestra que el proceso se ha tornado en irregular por haberse transgredido los derechos fundamentales que integran el debido proceso, esto es, el derecho de defensa; ello, a su vez, ha determinado la afectación de la tutela jurisdiccional, ambos garantizados por la Norma Constitucional."

[106] En dicha sentencia se lee: "Este Tribunal advierte que la sentencia condenatoria no determina con exactitud el momento en que ocurrieron los hechos que se le imputan al accionante, señalándose de forma genérica que participó el actor en atentados terroristas, entre ellos un paro armado ocurrido en 1991, y haber iniciado su participación en un organismo de fachada de Sendero Luminoso el mismo año, agregando, además, que el acusado se alejó de la subversión, sin indicar, sin embargo, el momento en que ello se produjo. Como es de verse, el órgano jurisdiccional penal no determinó con precisión el momento en que ocurrieron los hechos delictivos imputados, pese a que de ello dependía en gran medida el grado de afectación de la libertad individual del imputado."

según el auto apertorio de instrucción, obrante a fojas 92 de autos, se atribuye a "los denunciados Percy Escobar Lino y Víctor Raúl Martínez Candela, el hecho de haber resuelto los procesos de acción de amparo (principal y medida cautelar) contenido en el expediente número cuarenticuatro-noventiocho (...) y acción de cumplimiento (principal y medida cautelar) contenido en el expediente número ochocientos sesentiocho – noventiocho, respectivamente, seguido por la empresa Luchetti Sociedad Anónima contra la Municipalidad Provincial de Lima y el Concejo Distrital de Chorrillos, por indicaciones del ex asesor presidencial Vladimiro Montesinos Torres", agregando más adelante que "tales hechos se adecúan en lo previsto y sancionado en la hipótesis legal contenida en los artículos trescientos diecisiete, trescientos noventicinco y cuatrocientos dieciocho del Código Penal vigente". Así descritos los hechos imputados y la norma en la que éstos son subsumidos, permiten al accionante tener un pleno conocimiento de la imputación que se realiza en su contra, no vulnerándose su derecho de defensa."

El desarrollo de estos conceptos, de una manera más precisa, lo encontramos en las sentencias recaídas en los Exp. 8123-2005PHC/TC – Caso Nelson Jacob Gurman, Exp. No. 0174-2006-PHC/TC – Caso Jhon Mc. Carter y otros, Exp. No. 8125-2005-HC/TC – Caso Jeffrey Immelt y otros; en donde el Tribunal Constitucional al hacer una especial referencia a la falta de motivación del auto apertorio de instrucción, sostiene que se produce la afectación al derecho de defensa al no individualizarse la imputación que recae sobre los procesados. De este modo:

"Examinado el cuestionado auto de apertura de instrucción (f. 392), de conformidad con la Cuarta Disposición Final Transitoria de la Constitución, podemos afirmar que tal resolución no se adecúa en rigor a lo que estipulan, tanto los instrumentos jurídicos internacionales de derechos humanos como la Constitución y la ley procesal penal citados. No cabe duda de que el artículo 77 del Código de Procedimientos Penales ofrece los máximos resguardos para asegurar

que el imputado tome conocimiento de la acusación que contra él recae, al prescribir que "El *auto será motivado y contendrá en forma precisa los hechos denunciados, los elementos de prueba en que se funda la imputación*[107], la calificación de modo específico del delito o los delitos que se atribuyen al denunciado". [108]

"En otras palabras, la protección constitucional del derecho de defensa del justiciable supone, a la vez, la obligación de motivación del Juez penal al abrir instrucción. Esta no se colma únicamente con la puesta en conocimiento al sujeto pasivo de aquellos cargos que se le imputan, sino que comporta una ineludible exigencia, cual es que la acusación ha de ser cierta, no implícita, sino precisa, clara y expresa, Es decir, una descripción suficientemente detallada de los hechos considerados punibles que se imputan y del material probatorio en que se fundamentan, y no como en el presente caso, en que se advierte una acusación genérica e impersonalizada que limita o impide al procesado un pleno y adecuado ejercicio constitucional del derecho de defensa."

---

[107] Reiteramos, entonces, que el Juez penal debe –al abrir instrucción- precisar en detalle y de forma individualizada cuáles son los hechos que se imputa específicamente al procesado o a cada uno de los procesados; no puede hacerse de manera genérica para todos los inculpados o con fórmulas vacías de contenido como: ..."estando a las condiciones personales del procesado"... o ..."en atención a las pruebas que fluyen de autos"... (pero no se especifican cuáles) hacerlo de esta manera afecta gravemente el principio de presunción de inocencia y, por tanto, el debido proceso (derecho a la defensa por violación del principio de imputación necesaria). Al respecto, Juan Igartua Salvatierra, en su *La motivación de las sentencias y su ubicación en el texto constitucional – España*. Material de estudio del curso de Despacho Judicial e Interpretación Jurídica de la Facultad de Derecho de la UNMSM, afirma que ..."en ocasiones los tribunales, con la cita genérica de algunos precedentes suyos, intentan motivar algo sobre lo que no han dicho ni una palabra." Róger Zavaleta y otros, por su parte, en *Razonamiento Judicial*. Ed. Gaceta Jurídica. 1ª. Edición. Lima 2004, p.408, nos dice: "Típico de esta clase de vicio es cuando en las resoluciones se hace una mera descripción de los hechos sin relacionarlos con prueba alguna, así como hacen una vaga alusión a todas las pruebas aportadas al proceso, cuando asevera que un hecho está probado, pero no indica la fuente o prueba de tal afirmación, las que se apoyan en pruebas ilícitas, entre otras."

[108] Cfr. Roxin, Claus, y otros. *Derecho Penal y Derecho Penal Procesal*. Ed. Ariel. 1ª. Edición. España, marzo de 1989, p. 184, afirma que: "Para que haya un proceso penal propio de un Estado de Derecho es irrenunciable que el inculpado pueda tomar posición frente a los reproches formulados en su contra, y que se consideren en la obtención de la sentencia sus puntos de vista sometidos a discusión." Más adelante continúa: "La exposición del caso del inculpado sirve no sólo al interés individual de éste, sino también al hallazgo de la verdad. La meta procesal del esclarecimiento de la sospecha se alcanza en la mejor forma por medio de un proceso dialéctico, en el que se pongan a discusión aspectos inculpatorios y exculpatorios, así como argumentos y contrargumentos ponderados entre sí."

Del mismo modo, para apreciar cómo el principio de imputación necesaria guarda profunda relación con el derecho de defensa, de probar y presunción de inocencia, tenemos la siguiente ejecutoria suprema:[109] Exp.No.4468-2000-Lima, del 31.05.01, se lee: "Toda imputación hecha a nivel policial no ratificada en la etapa jurisdiccional y no corroborada con otros medios de prueba, carecen de mérito probatorio para acreditar la responsabilidad penal de la persona sometida a juicio; más aun atendiendo a que la doctrina procesal penal es objetiva al considerar que existe responsabilidad penal única y exclusivamente cuando existen en autos medios probatorios (testimoniales, reconocimiento, confrontaciones, peritajes, etc.) plurales y convergentes que acrediten en forma indubitable y fehaciente la responsabilidad penal del procesado."

Asimismo, queremos hacer mención a una sentencia expedida por el 42º. Juzgado Penal de Lima, Exp. No.013-2006-HC – Caso Edwin Ampuero Huamán, en la que –refiriéndose al principio de imputación necesaria- sostiene: ..."a fin de que cualquier procesado pueda hacer valer su derecho a la defensa, es indispensable que éste sepa cuáles son –de manera específica y concreta- los hechos que se le atribuyen y que presumiblemente constituyan delitos, puesto que ello le permitirá absolver cada uno de los cargos que se le imputan, proponiendo la actuación de pruebas que ayuden a su defensa, la actuación de los recursos que la ley procesal le franquea, como plantear excepciones o defensas previas, entre otros; en consecuencia, si no se precisa cuáles son los hechos supuestamente delictuosos que se atribuyen a una persona, ¿cómo podrá ejercer ésta adecuadamente su derecho a la defensa?"

[109] Sentencia extraída de la revista *Actualidad Jurídica, No.134,* Ed. Gaceta Jurídica, p. 130.

De otro lado, es de resaltar que el derecho de defensa es esencial en todo ordenamiento jurídico. Mediante él se protege una parte medular del debido proceso. Las partes en juicio deben estar en la posibilidad jurídica y fáctica de ser debidamente citadas, oídas y vencidas mediante prueba evidente y eficiente. Se pueden consignar, entonces, hasta tres características del derecho de defensa: a) Es un derecho constitucionalmente reconocido, cuyo desconocimiento invalida el proceso; b) Convergen en él una serie de principios procesales básicos, a saber: el principio de la inmediación, el derecho a un proceso justo y equilibrado, el derecho de asistencia profesionalizada y el derecho de no ser condenado en ausencia. c) Un punto central es el beneficio de gratuidad en juicio, que surge como consecuencia del principio de equidad. El juzgador debe garantizar que las partes en un proceso tengan una posición de equilibrio entre ellas; es decir, sin ventajas.[110]

Por su parte, José Camps Zeller[111], nos dice que en virtud de este derecho, a toda persona se le asegura…"la posibilidad de intervenir ya sea directamente y/o a través de un defensor letrado, desde el inicio y a lo largo de todo el procedimiento penal, en todas las actuaciones del procedimiento en que la ley expresamente no lo excluye, con la finalidad de manifestar su inocencia o cualquier otra circunstancia que extinga o atenúe su responsabilidad."

Carocca Pérez[112], advierte …"las dos dimensiones del derecho de defensa: a) como derecho subjetivo; y, b) como garantía del proceso. En lo que respecta a la primera dimensión, es visto como un derecho fundamental que pertenece a todas las partes en el proceso, cuyas notas características son su *irrenunciabilidad* (la parte no puede decidir que no se le conceda la oportunidad de defenderse) y su *inalienabilidad* (no puede ser dispuesta por su titular, ni su ejercicio puede serle

[110] Cfr. Bernales Ballesteros, Enrique. *La Constitución de 1993 – Análisis comparado…* p. 656 y ss
[111] Citado por Reyna Alfaro, Luis Miguel. *El proceso penal aplicado.* Ed. Gaceta Jurídica. 1ª. Edición. Lima, 2006, p. 225.
[112] Citado por San Martín Castro, César. *Derecho Procesal Penal…* pp. 119-120.

substraído ni traspasado a terceros). En cuanto a su segunda dimensión, de carácter objetivo institucional, la defensa constituye un verdadero requisito para la validez del proceso, siempre necesaria, aun al margen o por sobre la voluntad de la parte, para la validez del juicio. El derecho de defensa de toda persona nace, según el texto constitucional, desde que es citada o detenida por la autoridad. Ello significa que surge con la mera determinación del imputado: no hace falta que exista una decisión nominal o formal al respecto, basta que, de uno u otro modo, se le vincule con la comisión de un delito. Existiendo una imputación nace el derecho de defensa, lo que importa reconocer que el sujeto pasivo de la imputación tiene, en cuanto posibilidad procesal, el derecho de acceder al proceso o investigación preliminar, a ser oído por la autoridad en todas y cada una de las instancias en que la causa se desenvuelva."

Conforme se desprende de las lecturas de las sentencias que se trascriben a lo largo de este trabajo, es evidente que el derecho de defensa se yergue sobre todo el proceso penal -y aun antes, desde la etapa de investigación policial[113]- como un escudo, una garantía trascendental para que los justiciables no vean afectados sus derechos que incluso pueden ser originados por una actuación inapropiada de él mismo[114]; será el Juez Penal el obligado de calificar y señalar las imputaciones que en concreto, ciertas e individualizadamente se formulen contra el procesado por parte del Ministerio Público, pues los mismos van a ser la guía de todo el proceso

[113] A tenor del artículo 139 inciso 14 de la Constitución, esta protección comprende desde la etapa de la investigación policial o desde el momento de la detención de la persona.

[114] Roxin, Claus, y otros. *Derecho Penal y Derecho Penal Procesal*… pp.184-185, sostiene: "Con frecuencia el mismo inculpado no puede exponer su punto de vista en forma exigida, y tampoco, en absoluto, defender él mismo la función de un control de los órganos de la justicia. Esto depende muchas veces de que no está en situación de referir su opinión oralmente o por escrito. Ante todo, le falta el conocimiento necesario sobre las cuestiones jurídico-procesales y materiales. También está a menudo confundido por la situación del proceso penal, para él desacostumbrada, y por esto no se encuentra en condiciones de apreciar objetivamente las cosas. Si se encuentra el inculpado en prisión provisional, entonces está todavía más claramente limitado respecto a sus posibilidades de defensa, especialmente en lo relativo a investigar circunstancias exculpatorias. El inculpado no tiene normalmente, por lo tanto, ninguna oportunidad de triunfo ante el fiscal, formado jurídicamente, que dispone además de facultades coercitivas y del aparato investigatorio policiaco. (…) Por eso, en interés de la limpieza del proceso penal, así como del hallazgo de la verdad, es irrenunciable el que sea puesto al lado del inculpado, en todos los casos importantes, una persona correspondientemente formada: el defensor."

penal[115]. Así, el defensor sabrá cómo ejercer adecuadamente la defensa de su patrocinado, pudiendo ofrecer y actuar pruebas para enervar las de cargo o con el fin de mitigar su responsabilidad, el Juez sabrá lo que se va a investigar como hecho delictuoso y sólo se actuarán y debatirán las pruebas pertinentes, el Fiscal finalmente acusará, si así corresponda, la defensa expondrá sus alegatos finales, y el Juez emitirá sentencia sobre todo lo actuado, no pudiendo salirse de dicho marco legal y siempre bajo el manto protector del derecho a la efectiva defensa.[116]

Miguel Colmenero[117], justificando la importancia de la aparición temprana o desde la etapa de investigación policial o fiscal del abogado defensor, a fin que se haga efectiva el derecho de defensa del investigado, sostiene que esto es así en función de que en esa etapa no sólo se practican investigaciones y otras actuaciones que tienden a fijar posiciones respecto de la presentación de una acusación, o a asegurar la presencia del sospechoso ante la justicia, o a proteger a la víctima; sino también a identificar y asegurar los medios de prueba que van a permitir a las partes acusadoras y defensoras sostener sus respectivas posiciones. No puede ignorarse, además, que en ocasiones lo actuado antes del juicio oral resulta relevante a efectos de una sentencia condenatoria.

---

[115] Reyna Alfaro, Luis Miguel. *El proceso penal aplicado* … p.226, sostiene: "El derecho a una defensa material tiene como una de sus expresiones más trascendentes el derecho del ciudadano a ser informado de la existencia de la imputación penal en su contra, de conocer los estrictos términos de tal imputación y de saber cuál es el material probatorio en que esta se encuentra sustentada. El Tribunal Constitucional español, en sentencia del 30 de setiembre de 2002 (STC 170/2002) indica que el derecho a ser informado de la imputación: "Consiste en la exigencia constitucional de que el acusado tenga conocimiento previo de la acusación formulada contra él, en términos suficientemente determinados para poder defenderse de ella de manera contradictoria (…) convirtiéndose en un instrumento indispensable para poder ejercitar el derecho de defensa, pues mal puede defenderse de algo quien no sabe qué hechos en concreto se le imputan."

[116] Oña Navarro, *Cuadernos de Derecho Judicial – Constitución y garantías penales…* p. 168 sostiene: "Entre estas exigencias de un proceso justo, que a todos nos vinculan e interesan, el derecho de defensa aparece como una de las más trascendentes y decisivas para conseguir ese *desideratum,* porque, finalmente, permite garantizar el que la pretensión punitiva a la que el Estado como tal tiene derecho puede ejercitarse con la suficiente seguridad de que se puedan alcanzar los objetivos propios del *ius puniendo* –irrenunciables, sin duda, para un Estado de Derecho- pero al mismo tiempo con las elementales garantías de que los derechos de los afectados serán respetados y salvaguardados en la mejor y en la máxima forma posible y admisible."

[117] Oña Navarro, *Cuadernos de Derecho Judicial – Constitución y garantías penales…* p. 89.

Los instrumentos internacionales ponen énfasis en ámbitos específicos del derecho a la defensa. El artículo 11° de la Declaración Universal de Derechos Humanos insiste en que se aseguren a la persona todas las garantías necesarias para su defensa. A su vez, el artículo 14°, inciso 3, acápite "d" del Pacto Internacional de Derechos Civiles y Políticos considera pertinente requerir una defensa no sólo realizada a título personal, sino también a través de un abogado. Por su parte, el artículo 8°, inciso 2, acápite c de la Convención Americana sobre Derechos Humanos concede al inculpado el tiempo y medios convenientes para que prepare y realice su defensa.

Teniendo en cuenta tales dispositivos, conviene preguntarse cuándo se produce una violación del derecho de defensa. Ello ocurrirá cuando una persona no logra ofrecer a quien la juzga los elementos necesarios para desvirtuar una acusación en su contra o para afirmar que tiene la razón en lo que alega. Pero no todo acto que imposibilita un correcto uso de la defensa produce un agravio al derecho.[118]

3.3. BIEN JURÍDICO

3.3.1 El bien jurídico penal.

El altísimo grado de desconocimiento de las normas básicas de convivencia entre otros elementos produce en el comportamiento del hombre en sociedad encuentros y desencuentros con el derecho, de aquí por un lado la necesidad de que existan normas claras[119] para su cumplimiento y por otro, que las mismas sean difundidas a tiempo para que se conozcan y se respeten.

[118] Cfr. STC Exp. No. 6712-2005-HC/TC – Caso Magaly Medina Vela.
[119] Cfr. Schopenhauer, Arthur. *La Sabiduría de la Vida, en torno a la filosofía*. Editorial Porrúa, S.A. 2da. Edición, México 1991, p. 238.

Debemos tener presente que el bien jurídico es el aspecto fundamental en la dogmática penal moderna. El bien jurídico es reconocido como la base de la estructura, la interpretación de los tipos[120] y la clasificación de los distintos grupos de tipos penales en la parte especial de los códigos penales.

El bien jurídico se denomina de formas diversas, tales como: derecho protegido, bien garantizado, interés jurídicamente tutelado, objeto jurídico[121], núcleo del tipo, kernel[122], objeto de protección. No puede surgir el delito por inexistencia del objeto de tutela o por falta de idoneidad de la acción que hace imposible la lesión de un bien jurídico[123], el cual se presenta en las formas más diversas debido a su pretensión de garantizar los derechos de toda persona, como pueden ser entre otros: reales, jurídicos, psicológicos, físicos, etc.

Rocco precisó que el concepto de bien jurídico ha de apoyarse sobre la idea de valor[124]. Según Cobo del Rosal, el bien jurídico se puede definir como "todo valor de la vida humana protegida por el derecho"[125]. Para Jescheck el bien jurídico constituye el punto de partida y la idea que preside la formación del tipo. Afirma además que son bienes jurídicos aquellos intereses de la vida, de la comunidad a

---

[120] Cfr. Jescheck, Hans-Heinrich. *Tratado de Derecho Penal – Parte General.* Trad. Manzanares, Samaniego, Comares. Ed. Granada. España, p. 275.

[121] Cfr. Pisapia, Gian Doménico. *Instituzioni di Diritto Penale. Parte Generale e Parte Speciale*, Padova. Cedam. Casa editricce. Dott, Vicenza, 1965, p. 43. El autor, señala que, "por objeto jurídico del delito", se entiende generalmente, el bien o el interés protegido por la norma y la lesión o puesta en peligro con el delito.

[122] En informática, el núcleo (también conocido en español con el anglicismo *kernel*, de la raíz germánica *Kern*) es la parte fundamental de un sistema operativo.

[123] Cfr. Bettiol, Giuseppe. *Instituzioni di diritto e procedura penale. Principi Fondamentali del Diritto penale vigente,* terza edizione, Padova. Cedam. Casa Editrice, Bolonia, 1984. p. 78

[124] Cfr. Bettiol, Giussepe. *Instituzioni di diritto e procedura penale…* p. 84

[125] Cfr. Cobo Del Rosal, Manuel y Vives Antón. *Derecho penal. Parte general*, Edit. Tirant lo Blanch, Madrid, 1988, pp. 249.

los que presta protección el derecho penal[126]. Podemos afirmar, entonces, que no hay delito si no hay bien jurídico qué proteger.

El derecho penal moderno es producto de las ideas de la ilustración. El triunfo de las ideas políticas de la revolución francesa influyó decisivamente en el derecho; de las ideas de limitar el poder absoluto del monarca surge la limitación del poder punitivo del Estado[127]. A partir de entonces se entiende que la función de derecho penal es la protección de bienes jurídicos y que "la conducta humana solamente puede ser injusto punible si lesiona un bien jurídico"[128].

Los bienes jurídicos que tutela el derecho penal son los más necesitados de protección por el valor que representa el objeto de tutela como son la vida, la libertad, el patrimonio, la seguridad, la salud, libertad sexual, entre otros. El motor que produce la necesidad de crear y actualizar el derecho es la justicia. Siempre se ha reconocido que el fin del derecho es la justicia a partir de esta afirmación es que el tema cobra relevancia.

Los códigos decimonónicos, bajo la influencia del estado liberal, y del pensamiento del *laissez faire et laissez passer le monde va de lui même*[129] se ocuparon principalmente de la protección de intereses individuales; vida, libertad, patrimonio individual. Los códigos del siglo pasado iniciaron el camino hacia la protección de bienes

---

[126] Cfr. Jescheck Hans, Heinrich. *Tratado de derecho penal, parte general*. Traducción y adiciones de derecho penal español por Santiago Mir Puig y Francisco Muñoz Conde. Volumen I. Editorial Bosch, Barcelona 1981, p.350.

[127] "La idea de bien jurídico procede del pensamiento de la Ilustración y fue formulada y fundamentada por Feuerbach con la pretensión de separar Derecho y moral, y, en concreto, con la voluntad de excluir del ámbito del Derecho Penal las conductas meramente inmorales." Corcoy Bidasolo, Mirentxu. *Delitos de peligro y protección de bienes jurídicos supraindividuales*. Tirant lo blach, Valencia. 1999, p. 176.

[128] Cfr. Corcoy Bidasolo, Mirentxu. *Delitos de peligro y protección de bienes jurídicos supraindividuales* ... p.176.

[129] "Dejad hacer, dejad pasar, el mundo va solo" es una frase de Jean-Calude Marie Vicent de Gournay que resume la ideología liberal refiriéndose a la absoluta libertad en la economía sin intervención del Estado.

jurídicos colectivos, intervencionismo estatal, más acorde con una concepción del estado social de derecho en el que el estado regula la economía y el mercado.

Birnbaum, desde una perspectiva jusnaturalista moderada[130], realiza la primera formulación del concepto de bien jurídico estableciendo que los bienes jurídicos "están más allá del derecho". No obstante, es importante reconocer que desde esta inicial concepción jurídica positiva del bien jurídico se aprecia ya su carácter "limitador"[131] del poder punitivo del Estado. De acuerdo a Birnbaum, los bienes jurídicos tienen una concepción trascendente[132] pues se encuentran fuera del derecho. Son producidos por la naturaleza y el desarrollo social y el derecho simplemente se limita a reconocer su importancia e incorporarlos como objeto de protección.

Binding, desde el positivismo jurídico, reformula la tesis trascendentalista de Birnbaum. Para Binding "el bien jurídico queda establecido, no reconocido, dentro del contenido de la norma jurídica, es inmanente a la norma"[133]. En consecuencia, el bien jurídico no es un concepto metajurídico sino que se encuentra en la propia norma y Binding lo concibe como la "condición de la vida sana de la comunidad jurídica"[134]. En palabras de Bustos[135], "Binding une lesión jurídica con el bien jurídico". En definitiva nos dice el recordado profesor chileno "la teoría de que el delito es lesión de un bien jurídico".

Welzel propone un concepto trascendentalista del bien jurídico con un carácter limitador del ius puniendi. Adopta y supera la posición de Binding; la norma y el deber subyacente es lo significativo en el derecho penal pero Welzel encuentra que

---

[130] Cfr. Birnbaum, ciyado por Bustos, Juan. *Manual de Derecho Penal - Parte General*, 3ra Edición. Ed Ariel S.A. Barcelona, 1989. p. 45.
[131] Cfr. Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 46.
[132] Citado por Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 46.
[133] Citado por Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 46.
[134] Citado por Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 47.
[135] Cfr. Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 47.

el bien jurídico "no queda identificado con la norma y está más allá de ella[136]". El bien jurídico es entendido como los "deberes ético-sociales que sirven de base a las prohibiciones[137]". Sin embargo, el concepto de bien jurídico de Welzel tiene poca utilidad dogmática pues únicamente se le otorga la función de interpretación de los tipos particulares[138].

Jakobs desde su perspectiva funcionalista sistémica, retorna radicalmente al positivismo jurídico de Binding[139], niega totalmente la teoría del bien jurídico defendiendo, en su lugar la teoría de la validez de la norma.

La teoría de la validez de la norma ha cuestionado no solo el contenido de bien jurídico sino su propia existencia[140]. No obstante, el bien jurídico y su importancia en un derecho penal democrático se mantienen vigentes en el derecho penal contemporáneo[141]. La subsistencia del bien jurídico que sirva de límite material a la intervención punitiva estatal es coherente en el ordenamiento de sociedades democráticas regidas por el orden constitucional que respete la dignidad de la persona humana.

La constante lucha por controlar y limitar la respuesta estatal en defensa de los ciudadanos que se contrapone con la potestad punitiva del estado genera un permanente conflicto en las ciencias penales. Sin embargo, corresponde al bien jurídico penal, en un estado de derecho, restringir el poder punitivo del estado y

---

[136] Citado por Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 50.
[137] Citado por Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 50.
[138] Citado por Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 51.
[139] Citado por Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 47.
[140] Cfr. Hoy la capacidad y utilidad de la teoría del Bien Jurídico está siendo cuestionada por los penalistas que colocan en la base de sus propuestas el funcionalismo en su expresión más extrema: la teoría funcionalista sistémica de Luhmann. Si se asiente el funcionalismo sistémico con su postulado que la misión del derecho penal es asegurar por sobre todas las cosas simplemente la vigencia de la norma sin otra referencia material legitimadora que la defensa del sistema social. (Hormazabal p. 7)
[141] El bien jurídico se justifica como categoría límite al poder punitivo del Estado (...) las funciones de garantía son inherentes al bien jurídico penal y se vincula a la relación individuo-Estado. Cfr. Urquizo, José. El Bien Jurídico en Revista Peruana de Ciencias Penales, Nº 6, p. 825.

establecer los límites materiales que protejan eficazmente al individuo en concordancia con la misión del derecho penal de "protección de la convivencia en sociedad de las personas"[142]. El control estatal mediante el derecho penal se consiente, en palabras del profesor Urquizo: "La intervención del Derecho Penal se justifica como protección de bienes jurídicos.[143]"

En resumen, la teoría del bien jurídico aparece en el siglo antepasado con una clara inspiración liberal y con el declarado intento de limitar la obra del legislador penal[144], describe el elenco de hechos merecedores de pena únicamente a los socialmente dañosos.

3.3.2 Bienes jurídicos colectivos y Bienes jurídicos individuales.

El bien jurídico cumple una función esencial del derecho penal al establecer, a través de la protección de los bienes, el mínimo ético social necesario para la convivencia en opinión de la mayoría, de tal manera, que es necesario un equilibrio entre la protección de la sociedad y la de los individuos.

Todo *tipo penal* tiene un bien jurídico o varios.[145] Por ejemplo, en el delito de homicidio el bien que se tutela es la vida de los seres humanos, en tanto que en el delito de violación sexual, los bienes son el derecho la libertad sexual, a elegir de

[142] Cfr. Jescheck, Hans-Heinrich. *Tratado de Derecho Penal - Parte General*, Granada 2002 – España, p. 2. Este autor precisa que la finalidad del derecho penal es la protección de bienes jurídicos, bienes vitales imprescindibles para la vida en comunidad (p. 7).

[143] Cfr. Urquizo, José. *El Bien Jurídico Urquizo*… p. 824. El conflicto estado- individuo se percibe más nítidamente en sociedades latinoamericanas en las cuales la tentación totalitaria vence periódicamente algunos regímenes políticos, los cuales instrumentalizan el derecho penal para alcanzar sus fines. En este contexto la defensa de un concepto limitador del bien jurídico y del principio de legalidad resultan indispensables para controlar el desborde punitivo de un estado totalitario.

[144] Cfr. Antolisei, Francesco. Problema del bene giurídico. En: *Rivista Italiana di Diritto Penale*, Edit. Giuffre, Milano, 1939, pp. 3 y ss.

[145] Cfr. Bustos Ramírez. *Manual de derecho penal. Parte especial*. Edit. Ariel, Barcelona, 1982, p. 6. Este autor afirma que Hassemer y Padovani son los descubridores de los bienes jurídicos colectivos.

manera libre el lugar, momento y la apersona con la que se quiere entablar una relación de tipo sexual, de igual forma se protege el derecho al derecho al libre desarrollo del los menores de edad (indemnidad sexual), que se protegen mediante la determinación de un proceso de valoración de la conducta descrita. Esta protección es realizada normativamente mediante la prohibición de acciones cuyos contenidos son la materia descrita por la Ley Penal.

En el desarrollo del concepto de bien jurídico se ha diferenciado entre individuales y colectivos. Los bienes jurídicos individuales afectan directamente a la persona individual, en sus intereses particulares. Poseen un contenido eminentemente personal[146]. Por su parte, los bienes jurídicos colectivos afectan a la sociedad como tal, al sistema social que constituye la agrupación de varias personas.[147] A este tipo de bienes, Pisapia les ha denominado intereses de todos.[148]

El fundamento de los bienes jurídicos colectivos se sustenta en la realidad social y en el modelo de Estado social. Por una parte, existen nuevas necesidades sociales derivadas de la expansión de la tecnosfera concebida en el seno de la revolución industrial, técnica y científica, y que demandan su satisfacción, entre otros medios, a través de una eficaz protección jurídica para enfrentar esos riesgos de la modernidad.[149]

Pues bien, la atención de estas demandas tiene precisa acogida en el modelo de Estado social y democrático de derecho, en virtud del cual éste debe atender a las

[146] Cfr. Jescheck, Hans-Heinrich. *Tratado de Derecho Penal - Parte General*… p. 277
[147] Cfr. Muñoz Conde, Francisco. *Derecho Penal.* Ed. Tirant lo Blanch. 16ª. Edición. Valencia – España 2007, p. 65.
[148] Cfr. Pisapia, Gian Doménico. *Instituzioni di Diritto Penale. Parte Generale e Parte Speciale*…p.14.
[149] Cfr. Tiedemann, Klaus. *Lecciones de Derecho penal económico.* Barcelona. PPU 1993, pp.34-36.

necesidades de todos y cada uno de los miembros de la sociedad, con el objeto de tender hacia la libertad e igualdad material, razón que justifica una intervención estatal activa para promover la atención de dichas necesidades, superando las disfuncionalidades económicas y sociales.[150]

En nuestra opinión y como lo estaremos exponiendo posteriormente, los bienes jurídicos del delito informático son supraindividual. Los delitos de peligro y su vinculación a un bien jurídico supraindividual, podrá ser una mejor forma de evitación de las conductas definidas como delitos informáticos.[151]

3.3.3 El bien jurídico como objeto central de protección del Derecho Penal.

El derecho a penar[152] o sancionar se manifiesta a través del derecho penal con la imposición de la pena a las conductas que lesionen o pongan en peligro bienes jurídicos tutelados.

En consecuencia, la elaboración del concepto de bien jurídico se encuentra estrechamente vinculada al respeto de la dignidad humana como límite del poder punitivo del Estado. En palabras de Bustos, el bien jurídico "es una síntesis normativa determinada de una relación social concreta y dialéctica[153]". Esta concepción, que corresponde a un Estado democrático de derecho, es el producto de su evolución histórica que considera al respeto de la dignidad de la persona humana como el límite de la actividad punitiva del estado en una sociedad genuinamente sometida a los principios constitucionales.

---

[150] Cfr. Bustos Ramírez, Juan. *Los bienes jurídicos colectivos: control social y sistema penal*. PPU. Barcelona 1987, p.183 y ss.
[151] Cfr. Mazuelos, Julio. Delitos informáticos: Una aproximación a la regulación del CP peruano. En: *Revista Peruana de Doctrina y Jurisprudencia Penales*. N° 2. 2001. Ed. Grijley. p. 315.
[152] Cfr. Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 41.
[153] Cfr. Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 55.

Bustos señala que el concepto moderno de bien jurídico se debe definir en torno a la persona humana como ente social de una sociedad democrática[154]. Apunta, subrayando que se trata de un concepto en continua revisión y mutable de acuerdo a las necesidades sociales del individuo, que en definitiva "es una síntesis normativa determinada de una relación social concreta y dialéctica[155]". En consecuencia, el catálogo de bienes jurídicos variará de acuerdo a la evolución social. Se incorpora nuevos intereses y se dejará de lado otros que resulten innecesarios para la convivencia en sociedad. La valoración de la importancia de un interés socialmente relevante se efectúa en un instante histórico concreto. El bien jurídico penal surge de relaciones sociales concretas. "El bien jurídico en cuanto producto social es un producto histórico, por ello se puede afirmar que el bien jurídico es una "síntesis" alcanzada en un momento histórico cultural"[156].

En definitiva, el bien jurídico, sea concebido como "intereses de la comunidad cuya protección garantiza el derecho penal"[157] o como "presupuestos que la persona necesita para su autorrealización y el desarrollo de su personalidad en la vida social",[158] constituye el fundamento material del injusto[159] que cumple una doble función; limita al ius puniendi (fundamenta la intervención estatal y, a la vez, la deslegitima) y es una garantía para el ciudadano[160]. La intervención estatal, a través del derecho penal, sólo se justifica cuando se protege a la persona humana a través de la tutela penal de bienes jurídicos.

---

[154] Cfr. Bustos, Juan. *Manual de Derecho Penal - Parte General*… p. 54.
[155] Cfr. Bustos, Juan. *Manual de Derecho Penal - Parte General*… p.55.
[156] Urquizo p. 830. Muñoz Conde indica que se efectúa una valoración histórica teniendo en cuenta las necesidades sociales y las concepciones morales dominantes en la sociedad: "los valores que en cada época determinada el legislador somete a tutela penal" ob. cit. p. 66.
[157] Cfr. Jescheck, Hans-Heinrich. *Tratado de Derecho Penal – Parte General*… p. 274.
[158] Cfr. Muñoz Conde, Francisco. *Derecho Penal – Parte General*… p. 65.
[159] Cfr. Bustos, Juan. *Manual de Derecho Penal - Parte General*… p.49
[160] En este sentido, Bustos, Juan. *Manual de Derecho Penal - Parte General*… p.55 y Muñoz Conde, Francisco. *Derecho Penal – Parte General*… p.65.

3.3.4 El principio de lesividad de bienes jurídicos.

El artículo IV del Título Preliminar del Código Penal contiene el principio de lesividad de bienes jurídicos de acuerdo al cual solo se sancionan conductas capaces de poner en peligro o de lesionar bienes jurídicos. Cada tipo penal al proteger un bien jurídico en concreto establece un objeto de protección.

El principio de lesividad[161] establece que las conductas tipificadas deben proteger un bien jurídico en concreto. De acuerdo a este principio al presentarse una nueva manifestación criminal utilizando los avances tecnológicos debemos establecer, en primer lugar, si estas conductas afectan (usando nuevos medios) un bien jurídico ya tutelado o si nos encontramos ante un nuevo interés necesitado de protección en cuyo caso corresponde crear un nuevo tipo penal. Si constatamos que estas conductas afectan bienes jurídicos ya reconocidos por el derecho penal tendremos que adecuar los tipos penales existentes a las nuevas formas de comisión.

Desde una perspectiva constitucional, la delimitación de una conducta como antijurídica, es decir, aquella cuya comisión pueda dar lugar a una privación o restricción de la libertad personal, sólo será constitucionalmente válida si tiene como propósito la protección de bienes jurídicos constitucionalmente relevantes (*principio de lesividad*). Como resulta evidente, sólo la defensa de un valor o un interés constitucionalmente relevante podría justificar la restricción en el ejercicio de un derecho fundamental. "Por relevancia constitucional no ha de entenderse que el bien haya de estar concreta y explícitamente proclamado por la Norma Fundamental. Eso sí, habría de suponer una negación de las competencias propias del legislador ordinario. La Constitución contiene un sistema de valores compuesto por los derechos fundamentales, los derechos de los ciudadanos,

[161] Véase artículo VII del Título Preliminar del Código Penal.

aquellos que son necesarios y convenientes para hacer efectivos los fundamentales y los que simplemente se desprenden como desarrollo de aquellos. Por otra parte la interpretación que se realice de la Norma Fundamental no ha de ser estática sino dinámica; esto es adecuada a los cambios sociales y de cualquier otra índole que se vayan produciendo. De esta manera puede decirse que el derecho penal desarrolla, tutelándolos, los valores proclamados en la Constitución y los que de ella emanan; puede decirse, en fin, que detrás de cada precepto penal debe haber un valor con relevancia constitucional.[162]

3.3.5 El bien jurídico del delito informático.

A fin de establecer si con el uso de la informática se vulnera algún bien que deba ser elevado a la categoría de bien jurídico penal debemos, en primer término, identificar si las conductas que utilizan nuevas tecnologías o sistemas informáticos afectan bienes jurídicos ya tutelados o lesionan intereses nuevos que no son objeto de tutela; y, en segundo término, revisar si este nuevo interés cumple los requisitos de necesidad o merecimiento de protección penal[163] para ser reconocido por el derecho y elevado a la categoría de bien jurídico.

En la mayoría de los casos el uso de las nuevas tecnologías, especialmente la informática, lesiona diversos bienes jurídicos que ya se encuentran protegidos por el ordenamiento legal y, en muy escasas ocasiones, se constata que afecta a un nuevo interés jurídico. En el primer caso, la informática es solamente un medio para la comisión de conductas ya tipificadas[164] y, en el segundo caso, las conductas

[162] Cfr. STC Exp.00014-2006-PI/TC – Caso Colegio de Abogados Lima Norte.
[163] Silva Sánchez señala además que esta protección sea satisfactoria en términos de utilidad social. Silva Sánchez, J.M. *Aproximación al Derecho Penal Contemporáneo*, Barcelona, 1992, p. 289.
[164] En este caso, "sería más correcto hablar de criminalidad informática en cuanto nueva forma de comisión de delitos ya tradicionales:" Bramont Arias Torres, Luis. *El delito informático en el Código Penal Peruano*. PUC Fondo Editorial 1997. p. 58.

que utilizan medios tecnológicos al afectar el nuevo interés obliga elaborar un tipo penal que tutele adecuadamente al nuevo bien jurídico.

Cuando la informática es simplemente un medio para lesionar bienes jurídicos ya protegidos por el derecho encontramos, en ocasiones, que la nueva conducta es atípica[165] ya sea porque el tipo describe un medio específico de comisión o porque se establece una conducta imposible de ser realizada por la tecnología. En estos casos, a fin de respetar el principio de legalidad, se debe adecuar el tipo para comprender las nuevas formas de comisión. En otros casos, el tipo penal es suficiente para admitir las conductas que empleen la informática como medio de comisión. Sin embargo, el uso de elementos tecnológicos o informatizados en la comisión de un delito no es suficiente para denominar a la acción "delito informático", consideramos –pues- que la gran posibilidad de que los delitos sean cometidos a través de medios informáticos no puede generar *per se* toda una definición dogmática.

La construcción de un bien jurídico penal debe justificarse solamente cuando se cumplen los requisitos de ser merecedor de protección y necesitar la imposición de una pena. Es desde esta perspectiva que revisaremos si existe un nuevo bien jurídico que reúna estas características.

En este sentido, no comparto la necesidad de crear una categoría denominada delitos computacionales[166] pues casi todos los tipos previstos en el Código Penal

[165] El repentino uso de las nuevas tecnologías demostraron que algunos tipos penales no eran aptos para reprimir las nuevas conductas debido, principalmente, por la descripción cerrada del tipo. La transferencia no autorizada de fondos no podía ser tipificada como delito de hurto porque el objeto material "cosa mueble" entendida como objeto material no podía ser homologada con el concepto del dinero virtual; de otro lado, el delito de estafa tampoco podía comprender esta nueva conducta pues el concepto clásico de engaño estaba referido a una acción sobre una persona mientras que las transferencias electrónicas de fondos se trataba de manipulaciones en el sistema informático.

[166] "El delito computacional es aquella conducta que empleando tecnología de la información vulnera bienes jurídicos reconocidos penalmente" Cfr. Reyna Alfaro, Luis Miguel. *Los delitos informáticos*. Jurista Editores. Lima, enero 2002, p. 132.

pueden ser cometidos con el uso de elementos informáticos y esta definición no corresponde a una categoría jurídica debido que el criterio clasificador debe ser el bien jurídico y no el medio de comisión.

El bien jurídico que surja o se reconozca con el uso de la informática debe también cumplir los principios de última ratio, intervención mínima. Se debe recordar que no todos los bienes jurídicos merecen protección penal ni se debe proteger al bien jurídico de todos los ataques, sino solamente de los ataques más graves que pueda sufrir.

En cualquier intento de tipificar nuevas conductas se debe hacer una constatación previa de la existencia de un bien socialmente valioso merecedor de ser reconocido como bien jurídico, distinto a los ya tutelados y demostrar que merecen tutela penal porque son indispensables para mantener un sistema de convivencia estable.

Al intentar concretar el bien jurídico que se protege con el uso y difusión de las nuevas tecnologías, hay que tener en cuenta la importancia de la tecnología y, en especial, de la telemática en las relaciones sociales modernas. La irrupción y expansión de las nuevas tecnologías, especialmente de los sistemas informatizados y su interconexión mediante el internet, ha planteado la cuestión respecto a la existencia de un nuevo bien jurídico y cual sería específicamente el objeto de protección las conductas que utilizan las nuevas tecnologías.

Considero que la existencia de un verdadero delito informático debe sustentarse en la constatación de que hay un nuevo objeto merecedor de protección. Es decir, que se pueda demostrar que el uso de la tecnología o la informática afecta a un interés importante para mantener la coexistencia pacífica que no se encuentre protegido por el ordenamiento jurídico.

De acuerdo a Mazuelos[167]: "Los delitos informáticos presentan dos bienes jurídicos que pueden ser concebidos ampliamente respetando cada una de sus esferas de realización, atendiendo si la conducta incide sobre la intimidad de la persona (…) nada impide, sin embargo, que se reconozca la existencia de un bien jurídico supraindividual vinculado a la seguridad e intangibilidad del tráfico de información en la red y propendería a garantizar la libre participación de las personas (usuarios) en la red.

"Este bien jurídico supraindividual seguridad e intangibilidad del tráfico de información en la red se erige como un presupuesto objetivo depara la protección material de los bienes jurídicos interpersonales intimidad y patrimonio." [168]

Reyna ha propuesto que el nuevo bien jurídico penal a tutelar sería "la información como valor económico de empresa", el mismo que, a su juicio, cumple las exigencias de merecimiento de protección y necesidad de tutela[169].

La información con contenido patrimonial, datos sobre la intimidad, secretos industriales, secretos de estado, o activos contables, valor económico de la empresa insuficiente[170] si no se encuentra almacenada, tratada, sistematizada o circula en la net. Si la información (o data en términos informático) representa o contiene valor económico nos referimos en realidad al patrimonio o la seguridad de las comunicaciones informática y telemática.

[167] Cfr. Mazuelos, Julio. *Delitos informáticos: Una aproximación a la regulación del CP peruano*…p. 286.
[168] Cfr. Mazuelos, Julio. *Delitos informáticos: Una aproximación a la regulación del CP peruano*… p. 287.
[169] Cfr. Reyna Alfaro, Luis Miguel. *Los delitos informáticos*… p. 252.
[170] Cfr. Reyna Alfaro, Luis Miguel. *Los delitos informáticos*… p. 252.

3.3.6 Toma de posición.

Algunos trabajos que estudian las conductas nocivas que emplean la informática no han prestado la atención que merece el bien jurídico. Ocupan su atención en detalles absolutamente prácticos ofreciendo una casuística abrumadora de excesivas e innecesarias descripciones de las clases de virus que circulan en la red y presentan una extensa lista de las posibles formas de introducirse o alterar los datos en los sistemas informatizados.

Hay que tener en claro que los sistemas automatizados o informatizados almacenan, transmiten o tratan información (data). Esta información puede referirse a datos personales, patrimoniales, de seguridad del estado, de la empresa que refleja algún activo patrimonial diferente de información con contenido patrimonial.

En principio, considero que no resulta correcto que se pretenda definir al delito informático sobre la base del uso de elementos informáticos o vulnerando los derechos del titular de un elemento informático ya que sería una manera incorrecta de explicar el tipo penal en función al objeto material o sobre el cual se realiza la acción pues se requiere verificar si el bien jurídico propuesto cumple los requisitos exigidos por la doctrina. Así: necesidad de protección, importancia trascendencia para la vida moderna la seguridad o protección de datos informatizados o automatizados.

La seguridad de las comunicaciones e información informáticamente tratada o la seguridad de la información (o datos) que circulan en la red es el único que cumple los requisitos de necesidad de protección y merecimiento de pena y que, además, no se encuentra adecuadamente protegido en la legislación nacional o extranjera; razón por la que consideramos que éste es el bien jurídico a proteger.

La información, a secas, o la información que se encuentra fuera de un sistema informatizado no es el objeto específico de protección en las conductas que utilizan los sistemas informáticos. La información (almacenada o tratada fuera de los sistemas informatizados) tiene protección en los delitos contra la intimidad, la violación del secreto de las comunicaciones, violación del secreto profesional. En estos supuestos la información puede encontrarse en un soporte material, documento escrito o impreso. Aquí solo se protege específicamente a la información informáticamente tratada o almacenada en un soporte virtual, inmaterial o informático o que se encuentren en tránsito en cualquier sistema informatizado.

La protección de este nuevo bien debido a la especial importancia y trascendencia para la vida social, de este nuevo objeto de protección, es necesario adelantar las barreras de protección y tipificar la conducta como delito de peligro. Es conveniente sancionar las conductas de intrusismo o acceso ilegal o acceso no autorizado a los sistemas informatizados o bases de datos. Ello por la importancia de la información que circula o es almacenada en la red, razón que justifica el dar seguridad a este tráfico de datos cada vez más importante en una sociedad cada vez más informatizada.[171]

En consecuencia, las conductas que utilicen sistemas informáticos como simple medio de comisión, pero que vulneren bienes jurídicos ya tutelados, pueden ser objeto de reforma para adecuar el tipo para evitar las lagunas de punibilidad y ajustarse a las exigencias del principio de legalidad pero no deben denominarse, en estricto, delitos informáticos.

[171] Cfr. Gutierrez Frances, Mariluz. "Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa". En: *Estudios de Derecho Penal Económico*. Edición de Luis Arroyo Zapatero y Klaus Tiedeman. Ediciones de la Universidad de Castilla – La Mancha. 1994.

4. LA CRIMINALIDAD INFORMÁTICA Y EL CÓDIGO PENAL

4.1. Delitos afectados por la criminalidad informática.

Adicionalmente al surgimiento del nuevo bien jurídico merecedor de protección la informática y las nuevas tecnologías atraviesan todo el código penal[172]. Las tecnologías y la informática se pueden utilizar también para cometer conductas ilícitas ya tipificadas en el código penal como los delitos contra la intimidad y contra la libertad o indemnidad sexual. Con mucha frecuencia se amenaza con difundir fotos o videos íntimos a cambio de una suma de dinero o favores sexuales. También se ha detectado la difusión en la Internet de información o comentarios que afectan el honor de una persona o denigran la reputación comercial de alguna empresa.

[172] Rojas, por su parte, considera que "la relevancia penal de los comportamientos informáticos gira en torno a tres ejes fundamentales: el manejo de la información, las transferencias económicas en sentido virtual y la destrucción de los sistemas de datos." No obstante, como se verifica en las siguientes páginas, la informática puede ser un medio absolutamente capaz e idóneo para lesionar casi todos las bienes jurídicos tutelados en el Código Penal.

La difusión de la Internet también ha favorecido la actuación de pedófilos quienes amparados en el anonimato que le proporciona la red difunden pronografía y se contactan con los menores primero a través de la web cam y después incluso logran contactarse personalmente con los menores. En la mayoría de los casos, se necesita reformar los tipos penales para que sean aptos de subsumirse estas conductas.

Por cierto, la tecnología afecta especialmente al patrimonio, a través del fraude, con la manipulación de sistemas informático; operaciones fraudulentas por internet, la clonación de tarjetas y hurto de fondos. La libertad individual y sexual mediante la Extorsión como cuando se amenaza por e-mail. O más precisamente el chantaje sexual y económico cuando el delincuente logra captar, mediante la web cam, imágenes íntimas de la víctima con las cuales le obliga a dar una suma de dinero o un favor sexual. Por otro lado, se vulnera la intimidad y pueden constituir actos preparatorios de conductas más graves con las intrusiones (Hacking,) y el acceso y comercialización no autorizados a base de datos

El honor, en los tiempos de la informática, es afectado a través de los correos electrónicos o con publicaciones injuriantes en las páginas web. La internet es el medio preferido por los pedófilos para traficar con pornografía infantil ya que les permite mayor difusión y anonimato.

Veamos los siguientes:

4.1.1. Delitos contra el honor

> **Difamación.**
> **Artículo 132.-** El que, ante varias personas, reunidas o separadas, pero de manera que pueda difundirse la noticia, atribuye a una persona, un hecho, una cualidad o una conducta que pueda perjudicar su honor o reputación, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a ciento veinte días-multa.

> Si la difamación se refiere al hecho previsto en el artículo 131º, la pena será privativa de libertad no menor de uno ni mayor de dos años con noventa a ciento veinte días-multa.
>
> Si el delito se comete por medio del libro, la prensa u otro medio de comunicación social, la pena será privativa de libertad no menor de uno ni mayor de tres años y de ciento veinte a trescientos sesenticinco días-multa.

Bien jurídico.

El honor se encuentra protegido desde la norma constitucional en su artículo 2.7 en el cual se consagra como derecho fundamental de toda persona humana "el honor y la buena reputación" sin embargo, se trata de un concepto cuyo contenido ha variado dependiendo la época y el lugar.

El Bien Jurídico en este delito es el Honor que, a decir de la posición jurídica constitucional del profesor Ignacio Berdugo Gomez de la Torre *"está constituido por las relaciones de reconocimiento entre los distintos miembros de la comunidad, que emanan de la dignidad y del libre desarrollo de la personalidad. Estas relaciones actúan como presupuestos de la participación del individuo en el sistema social y precisamente parte de su contenido será consecuencia directa de su participación en el sistema social".* [173]

Urquizo Olaechea sostiene que la norma penal tutela "la dignidad de la persona humana"[174]. A partir de esta concepción se desprende que el titular del bien jurídico tanto la persona natural o física como la persona jurídica[175].

---

[173] Cfr. Berdugo Gomes de la Torre, Ignacio. *Honor y Libertad de expresión*. Editorial TECNOS, 1987, Madrid - España, p.57. Cfr. Bramont Arias Torres, Luis Alberto y García Cantizano, María del Carmen. Manual de Derecho penal. Parte Especial. 3ra Edición. Ed. San Marcos, p.135.

[174] Cfr. Urquizo Olaechea, José. *Los delitos contra el honor en el nuevo Código Penal*, en RPCP Nº 1, Lima 1993, p.235.

[175] Cfr. Bramont Arias Torres y García Cantizano. *Manual de Derecho penal*… p.136.

En la actualidad se vincula el honor como expresión del libre desarrollo de la personalidad a partir del cual únicamente se puede subsumir las conductas prevista en cualquiera de los tipos penales es verificando su idoneidad objetiva para suscitar el desprecio de los demás miembros de la comunidad[176].

De acuerdo a lo expresado por la doctrina, el honor, como objeto de protección en el delito de difamación, emana de la dignidad de la persona humana como sujeto de derecho vinculado al libre desarrollo de la personalidad. Bajo estos preceptos se elabora una concepción estrictamente jurídica de honor sobre la noción de *dignidad* de la persona.

Desde esta óptica, se atribuye al honor dos aspectos complementarios: uno *interno*, ideal e intangible vinculado con la dignidad de la persona como ser racional, y otro *externo,* relativo a su fama o reputación, es decir, por el juicio que la comunidad proyecta sobre el individuo[177]. Se designan dos dimensiones distintas: lo que cada uno piensa de sí mismo (sentido subjetivo) y la reputación y estimación respecto del entorno y círculo social (sentido objetivo) que afecta las relaciones y el desarrollo de las personas en la dinámica social.

El profesor Roy Freyre[178] enseña que la doctrina y la jurisprudencia nacional "han tomado en consideración los aspectos subjetivo y objetivo del honor para tipificar,

[176] Cfr. Laurenzo Copello, Patricia. *El bien jurídico en los delitos contra el honor*, en Revista Peruana de Ciencias Penales Nº 12, p. 55.

[177] Cfr. Salgado Carmona, Concepción. Delitos contra el honor. En: Cobo del Rosal, Manuel (Dir): *Curso de Derecho penal español* - Parte especial I, Marcial Pons, Madrid, 1996, pp. 464-465.
[178] Cfr. Roy Freyre, Luis. Derecho Penal. Tomo I, Parte Especial. 2da Ed., p. 427.

interpretar y juzgar los hechos los hechos que pudieran afectar o lesionar dicho bien jurídico."

Elementos objetivos.

La conducta central de este delito es "atribuir"[179] que consiste en realizar actos de desmerecimiento respecto del sujeto pasivo, a quien se descalificará atribuyéndole hechos (sucesos o acontecimientos), cualidades (calidad personal), o conductas (modo de proceder).

La difamación es una injuria que se difunde otras personas[180]. Esto es, sujeto activo difunde la conducta, cualidad o hecho ante un grupo de personas de tal manera que se difunda o sea conocida por más de dos personas.

Roy Freyre[181], precisa que la expresión "*que pueda perjudicar el honor o reputación*" significa que solo se requiere la probabilidad de producir un perjuicio y no es necesario que se produzca el daño o lesión al honor en concreto. De esta manera, el Código Penal peruano tutela el honor en manifestación objetiva en la difamación; en el aspecto subjetivo con la injuria y en la calumnia que tutela la manifestación objetiva y subjetiva.

Aspecto Sujetivo.

En el apecto subjetivo se trata de ilícito eminentemente doloso. El agente debe actuar con la evidente intención de afectar el honor de otra persona endilgándole conductas que desmerezcan su buena reputación.

[179] Cfr. Bramont Arias Torres y García Cantizano. *Manual de Derecho Penal – Parte Especial*… p. 141.
[180] Cfr. Bramont Arias Torres y García Cantizano. *Manual de Derecho penal – Parte especial*… p.141.
[181] Cfr. Roy Freyre, Luis. *Derecho Penal, T I, Parte Especial*… p. 300.

Difamación agravada

El mayor disvalor de la acción se refiere a la extensión de la difusión del agravio; esto es, por imputar conductas delictivas, o por difundir los agravios a través de un medio de prensa.

Existe mayor desvalor de la acción por la capacidad de difundirse el agravio a una extensa cantidad de personas a través de la prensa, referido a los medios impresos como los periódicos, u otros de medios de comunicación que tradicionalmente eran la radio o televisión, en los cuales el responsable de la publicación era fácilmente identificable como el autor de la nota, el editor o el director del medio. Sin embargo, el desarrollo de la informática ha incorporado nuevos medios que cumplen, incluso más eficazmente, la función de difundir, a través del internet, cualquier clase de información contenida en texto, video o imagen.

Por cierto, los medios informáticos, redes sociales, correos electrónicos, twitter, blog o páginas web reúnen dos características centrales para propagar las noticias como es; i) capacidad de soportar archivos con información en cualquier formato sea audio, escritos o video y ii) difusión que incluso es mayor que los medio clásico de información pues con su publicación en una web o en un blog la noticia o comentario es capaz de ser visto por un número indeterminado de personas.

Finalmente convendría efectuar una modificación del delito de difamación para incluir todas las posibilidades de cometerse por médios informáticos como las redes sociales, que no pueden ser considerados como "medios de comunicación social". Así como, los twiters o los correos son enviados masivamente y

directamente a los usuarios quienes acceden a ellos desde sus computadoras o sus teléfonos móviles.

4.1. Delitos contra la intimidad.

4.1.2.1. Violación de la intimidad.

> **Artículo 154.-** El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años.
>
> La pena será no menor de uno ni mayor de tres años y de treinta a ciento veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista.
>
> Si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa.

Bien jurídico

Se protege la "intimidad personal[182]", reconocida en el artículo 2, inciso 7 de la Constitución, que comprenden los aspectos privados o reservados de una persona, a su familia o su círculo íntimo los cuales sólo pueden ser revelados por su autorización. Para Vives[183] la intimidad "las manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados a su titular sobre las que ejerce alguna forma de control cuando se ven implicado terceros."

[182] Cfr. Bramont Arias Torres y García Cantizano. *Manual de Derecho penal – Parte especial*… p.196.
[183] Cfr. Vives Antón TS y otros. Derecho Penal Parte Especial. Tirant lo blanch. Barcelona. p. 254.

Aspecto objetivo.

La violación de la intimidad se encuentra definida como el acceso o interferencia, indebida, de aspectos de la intimidad personal mediante instrumentos o procesos técnicos que permita observar o registrar hechos o imágenes. La norma establece que el medio o la vía para violar la intimidad estan referidos a procesos técnicos, instrumentos u otros medios entre los cuales, como correctamente señalan Bramont Arias Torres y García Cantizano, se econtrarían la informática y las nuevas tecnologías[184].

Resulta de singular importancia resaltar que en el caso que se acceda o conozca aspectos de la intimidad personal sin utilizar medios técnicos o instrumentos, la conducta resultaría atípica.

Las intromisiones ilegítimas en la esfera de la intimidad que queda directamente y exclusivamente reservada al propio interesado, quien tiene en sus manos la decisión sobre la magnitud del ámbito protegido.[185]

Conducta agravada.

El concepto de "medio de comunicación social" puede ser interpretado tal como se ha efectuado en la difamación agravada para incluir todas las formas de comunicación o difusión de información a través de la internet o las redes sociales.

El uso del medio de comunicación está referido a la divulgación de los aspectos de la intimidad personal o familiar.

[184] Cfr. Bramont Arias Torres y García Cantizano. *Manual de Derecho penal – Parte especial*… p.197.
[185] Cfr. Romeo Casabona, Carlos. *Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías*. En: Poder Judicial. Número 31. Setiembre 1993, p.166.

Consumación.

Se trata de un delito de resultado[186] ya que es necesario que se realice las conductas descritas como observar, escuchar o registrar aspectos de la intimidad. Todos los actos anteriores tendientes para acceder a la intimidad ajena se consideran tentativa.

4.1.2.2. Organización indebida de archivos.

> **Artículo 157.-** El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.
>
> Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36º, incisos 1, 2 y 4.

Aspecto objetivo.

Organizar. Se refiere a crear el archivo. Es decir, organizar u ordenar los datos de manera sistemática que facilita su rápida ubicación o la inmediata recuperación de éstos.

Proporcionar. Es entregar o poner a disposición de otros la información sobre la información personal contenida en los archivos

Emplear equivale a utilizar un archivo para extraer información de otra persona. En las modalidades de proporcionar o emplear

Estas conductas se encuentran relacionadas con la obtención indebida de datos sobre la intimidad personal prevista en el artículo 154 ya que en este tipo penal se

[186] Cfr. Bramont Arias Torres y García Cantizano. *Manual de Derecho penal – Parte Especial*… p. 198.

sanciona al que utiliza u organiza archivos con datos información personal que han sido extraídas por otro[187].

Sin embargo, el concepto "archivo", de acuerdo a la RAE, se refiere al "conjunto ordenado de documentos" lo cual implica que los datos de la intimidad personal se encuentre compilado u organizado con lo cual se excluye el uso de un dato o información suelta.

Las modalidades admiten el uso de la tecnología o la informática para crear el archivo, para extraer la información o difundirla. Sin embargo, consideramos necsario agregarse este extremo.

Objeto material.

Se refiere a "archivos" o datos organizados de manera sistemática y orgánica. Este concepto permite incluir a los archivos informatizados o almacenados en sistemas informáticos. Sin embargo, hay que tener en cuenta que los archivos deben contener, en concreto, información referida "a las convicciones políticas o religiosas y otros aspectos de la vida íntima". Esto es, por ejemplo, datos respecto a la orientación sexual o algún tipo de enfermedades.

4.1.3. Contra el secreto de las comunicaciones.

4.1.3.1 Apertura o apoderamiento de correspondencia.

> **Artículo 161.-** El que abre, indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico u otro documento de naturaleza análoga, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a noventa días-multa.

[187] Cfr. Bramont Arias Torres / García Cantizano, María. *Manual de Derecho Penal*… p. 201.

Bien jurídico.

Se da protección penal al derecho constitucional reconocido en el artículo 2, inciso 10 de la Constitución Política del Perú que reconoce el derecho fundamental al secreto y a la involabilidad de las comunicaciones y documentos privados.

Sujeto activo

Puede ser cualquier persona sin ninguna cualidad especial.

Aspecto objetivo

Abrir se refiere a tener acceso al contenido de alguna comunicación o misiva ya sea simplemente leyéndola o enterándose del contenido. Bramont Arias Torres y García Cantizano puntualizan que es necesario que la correspondencia se encuentre cerrada por cualquier medio para poder realizar la conducta requerida[188].

Apoderar tomándola materialmente de ésta para sí. Por cierto, las conductas centrales de este tipo penal se refieren a actos de apertura del envoltorio que contiene la misiva y de apoderamiento material de las comunicaciones al incorporar la correspondencia a su esfera de custodia[189].

Por cierto, este tipo penal no requiere que el agente divulgue la información que contiene la correspondencia.

[188] Cfr. Bramont Arias Torres y García Cantizano, María. *Manual de Derecho penal…* p. 210.
[189] Cfr. Bramont Arias Torres y García Cantizano, María. *Manual de Derecho penal…* p. 210.

Indebidamente

Este elemento normativo del tipo se refiere que el agente que abre o se apodera de la correspondencia no es el destinatario o no se encuentra autorizado a abrir las cartas. Por cierto, la autorización o el consentimiento del sujeto pasivo o el actuar por mandato de la ley[190] constituye una causa de atipicidad de la conducta.

Objeto material.

La conducta descrita como abrir o apoderarse debe recaer sobre una carta, pliego, telegrama, radiograma u otro documento de naturaleza análoga[191]. Esto es, que la norma nos proporciona un concepto restringido de misiva cuyo contenido deba estar impresa en un papel el cual pueda ser objeto de apoderamiento o de apertura. En este concepto se puede incluir los mensajes de correo electrónico cuando han sido impresos, pero se excluyen a éstos cuando se encuentran en tránsito, en el buzón de entrada o en la pantalla de la computadora.

En este caso, el objeto material estrictamente referido a una comunicación impresa limita la aplicación de este artículo a las conductas que utilizan la informática referida a la interceptación de comunicaciones vía la internet o las tecnologías de información.

En general el objeto material en los delitos referidos a la "Violación del secreto de las comunicaciones" (artículo 161), "supresión o extravío de correspondencia" (artículo 163) y "Publicación indebida de correspondencia" (artÏculo 164) son las comunicaciones que tienen como soporte el papel y no pueden extender este concepto a los medios tecnologícos o informáticos.

---

[190] Cfr. Bramont Arias Torres y García Cantizano se refieren cuando la apertura o apoderamiento de la correspondencia se efectua por mandato regular de un Juez. Cfr. *Manual de Derecho penal*… p. 211.

[191] Cfr. Bramont Arias Torres y García Cantizano Manual.., p. 211.

Asimismo, los elementos del tipo objetivo "abrir" o "apoderarse" se encuentran vinculados al apoderamiento material, pues indica la acción de tomar o aprehender el papel que contiene la carta u otro mensaje.

Sin embargo, la informática y las tecnologías de información (TICs) que utilizan la informática, la internet y las telecomunicaciones a través de las cuales se puede difundir, con mayor rapidez, eficacia y a muchas más personas pero no son impresas sino son transmitidas electrónicamente y son recuperadas o leídas en diversos tipos de aparatos o reproductores.

La principal limitación para adecuar a estos tipos penales para reprimir las manifestaciones de la delincuencia tecnológica es el objeto material. Estos delitos se configuraron sobre la base de que las comunicaciones se efectuaban básicamente mediante el papel y las nuevas formas de comunicación que se utilizan en las redes sociales como los mensajes de Facebook, el twiter etc. no puede asimilarse a este concepto tan limitado como es el papel pues no cabe una interpretación analógica. En este caso, estamos evidentemente ante una laguna de punibilidad pues aunque el tipo penal indica que se trata de documentos de "naturaleza análoga" se refiere únicamente a aquellos que tienen como soporte el papel; es decir que el tipo penal protege únicamente a las cosas corporales o tangibles.

Entonces, únicamente se podrá proteger la comunicación efectuadas por medios informáticos sólo cuando se han impreso y se encuentran en sobre papel.

En consecuencia, corresponde modificar este tipo penal para incluir en el objeto material a las comunicaciones interpersonales que se realicen por cualquier medio que utilice la informática y las tecnologías de información (TICs).

Aspecto subjetivo.

Es eminentemente doloso. El agente realiza las conductas de abrir o apoderar con el conocimiento específico que no es el destinatario de las comunicaciones.

Consumación.

El delito se consuma al realizar las conductas descritas ya sea abrir o apoderarse la correspondencia aunque el agente no llegue a conocer los elementos privados de la intimidad personal.

4.1.3.2. Escuchas indebidas.

> **Artículo 162.-** El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.
>
> Si el agente es funcionario público, la pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitado conforme al artículo 36º, incisos 1, 2 y 4.

Sujeto activo

Puede ser cualquier persona. En la agravante se requiere que el agente sea un funcionario público.

Aspecto objetivo.

Interferir se refiere a interrumpir, obstaculizar o dificultar las comunicaciones entre dos o más personas. Cuando se interfiere una conversación no es necesario

que el agente escuche la conversación pues basta con que se estorbe o interrumpa las comunicaciones.

Escuchar se refiere a tomar conocimiento de la conversación. Esto es oir el contenido de ésta[192].

Objeto Material

La norma señala que el objeto material es una "*conversación telefónica o similar*" lo cual restringe a las comunicaciones por voz pues se refiere las comunicaciones similares entre las que únicamente pueden ser las transmisiones de voz. En consecuencia, se excluyen otras transmisiones que se realizan con las nuevas tecnologías de información.

4.1.3.3. Supresión o extravío de correspondencia.

> **Artículo 163**.- El que, indebidamente, suprime o extravía de su destino una correspondencia epistolar o telegráfica, aunque no la haya violado, será reprimido con prestación de servicio comunitario de veinte a cincuentidós jornadas.

Sujeto activo.

Puede ser cualquier persona. No se exige calidad especial alguna.

Aspecto objetivo

Suprimir se refiere a eliminar o destruir totalmente la misiva. Esto es, hacer desaparecer la carta[193].

---

[192] Cfr. Bramont Arias Torres y García Cantizano, María. *Manual de Derecho penal*… p. 213.

[193] Cfr. Bramont Arias y García Cantizano consideran que no es necesaria la destrucción de la correspondencia. Sin embargo, considero que si el agente oculta la correspondencia estaríamos en el supuesto de extraviar, pues desde la perspectiva del destinatario éste no conoce la ubicación de la misiva. Cfr. Manual de Derecho penal… p.216.

Extraviar significa que el agente logre que la correspondencia se pierda o se desvíe de su destino impidiendo que llegue a manos del destinatario.

Objeto material.

Se restringe a la "correspondencia epistolar o telegráfica" como el objeto sobre el cual recae la acción. Esto es que los actos de supresión o extravío solo pueden recaer en comunicaciones escritas como cartas o mensajes. Las comunicaciones telegráficas transmiten mensaje utilizando señales eléctricas mediante líneas alámbricas o radiales. Los impulsos eléctricos son enviados empleando un código de líneas o puntos al receptor quien al recibirlo lo descodifica.

Como se puede apreciar este objeto material no incluye a los medios modernos de comunicación que han sido introducido por la informática o las tecnologías de la información por lo que se requiere su adecuación para cautelar debidamente todas las formas modernas de comunicación.

Adicionalmente, se debe tener en cuenta que estos medios de comunicación tienen muy poco uso en la actualidad.

4.1.3.4. Publicación indebida de correspondencia.

> **Artículo 164.-** El que publica, indebidamente, una correspondencia epistolar o telegráfica, no destinada a la publicidad, aunque le haya sido dirigida, será reprimido, si el hecho causa algún perjuicio a otro, con limitación de días libres de veinte a cincuentidós jornadas.

Sujeto activo.

Puede ser cualquier persona. No se exige calidad especial alguna.

Aspecto objetivo

La conducta de publicar se refiere a divulgar o difundir de manera pública o que puede ser conocida por un número indeterminado de personas[194]. Se sanciona la publicidad de la correspondencia que no ha estado destinada a este fin.

La publicación o difusión de la correspondencia puede efectuarse por cualquier medio capaz de poner a disposición de más de dos personas su contenido. Por lo tanto se pueden incluir los medios tecnológicos o informáticos para alcanzar tal fin.

La conducta debe realizarse sin autorización o justificación alguna.

Finalmente, se requiere de una condición objetiva de punibilidad que la publicación cause concreta y efectivamente un perjuicio de cualquier índole; moral o económico.

Objeto material.

Al igual que en el artículo 163 se limite el objeto sobre el cual recae la acción a la "correspondencia epistolar o telegráfica". Por cierto, estas conductas están redactadas sobre la base de proteger las comunicaciones que se realizan por medios tradicionales como la carta o el telegrama cuyo contenido se plasman siempre en un documento.

Consumación.

Al momento de ocasionarse el perjuicio proveniente de la publicación de la misiva

[194] Cfr. Bramont Arias y García Cantizano, María. *Manual de Derecho penal*… p. 217.

4.1.4. Ofensas al pudor público

4.1.4.1. Promoción del turismo sexual infantil a través de medios informáticos.

> **Artículo 181-A.- Turismo sexual comercial infantil y adolescente en ámbito de turismo**.
> El que promueve, publicita, favorece o facilita la explotación sexual comercial en el ámbito del turismo, a través de cualquier medio escrito, folleto, impreso, visual, audible, electrónico, magnético o a través de internet, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de catorce (14) y menos de dieciocho (18) años de edad será reprimido con pena privativa de libertad no menor de cuatro (4) mi mayor de ocho (8) años.
>
> Si la víctima es menor de catorce años, el agente, será reprimido con pena privativa de libertad no menor de seis (6) ni mayor de ocho (8) años.
>
> Será no menor de ocho (8) ni mayor de diez (10) años de pena privativa de la libertad cuando ha sido cometido por autoridad pública, sus ascendientes, maestro o persona que ha tenido a su cuidado por cualquier título a la víctima.

Sujeto activo.

Puede ser cualquier persona.

Elementos objetivos.

Promover es iniciar o impulsar algo, procurando su logro, es fomentar el ilícito penal. El legislador ha incluido las conductas sinónimas de favorecer o facilitar para describir el supuesto de hecho. Por cierto, favorecer significa prestar ayuda a otro para conseguir una cosa y facilitar es contribuir o ayudar en la ejecución de algo.

La publicidad, esto es el acto de difundir o impulsar algo, es una forma de promover o favorecer a través de la propaganda, anuncio o mensaje.

Por otra parte, se trata de promover o publicitar concretamente la prostitución de menores o el comercio sexual infantil entre 14 y 18 años[195]. En este caso, no se esta sancionando al proxenta sino al que lo ayuda a promover, difundir o publicita esta actividad.

Considero que debería existir una agravante cuando el menor tiene menos de 14 años pues es una conducta más repochable y el daño al niño es mucho mayor.

Hay que tener presente que los actos de promoción o favorecimiento de la explotación sexual comercial concretamente en el ámbito del turismo. De acuerdo al diccionario de la Real Academia de la Lengua Española turismo significa la "actividad o hecho de viajar por placer"; para Organización Mundial del Turismo "comprende las actividades que realizan las personas durante sus viajes y estancias en lugares distintos al de su entorno habitual…". De acuerdo a estas definiciones significa que el agente publicita o favorece el comercio sexual infantil a un turista o una persona que no resida en la localidad donde se realizan el comercio carnal.

Objeto material

Se refieren de manera bastante amplia a los medios utilizados para publicitar o difundir. Entre ellos se encuentran los medios de difusión que utilizan la internet aunque sería conveniente realizar una modificación para incluir cualquier forma de comunicación que utilice las tecnologías de la información.

[195] De acuerdo a los informes oficiales el comercio sexual infantil se ha incrementado en el Perú especialmente en las zonas del oriente peruano. En algunos casos, esta actividad se publicita a través de páginas web de agencias turísticas que ofrecen paquetes clandestinos Cfr. Red Peruana contra la Pornografía Infantil. www.red.org.pe.

4.1.4.2. Publicidad de prostitución sexual infantil

> **Artículo 182º-A.- Publicación en los medios de comunicación sobre delitos de libertad sexual a menores**.
> Los gerentes o responsables de las publicaciones o ediciones a transmitirse a través de los medios de comunicación masivos que publiciten la prostitución infantil, el turismo sexual infantil o la trata de menores de dieciocho años de edad serán reprimidos con pena privativa de la libertad no menor de dos ni mayor de seis años.
> El agente también será sancionado con inhabilitación conforme al inciso 4 del artículo 36º y con trescientos sesenta días multa.

Sujeto activo

Solo pueden ser los gerentes o responsables de las publicaciones de medios de comunicaciones masivas.

Tipicidad objetiva.

La conducta está referida a responsabilizar a los gerentes o editores de los medios de comunicación masiva que publiciten o promuevan la prostitución infantil o turismo sexual de menores. Por ello, se impone el deber de control de la publicidad que se incluya en cada emisión para evitar que se incluyan avisos que puedan servir de publicidad de estas conductas.

La norma señala que la publicación debe realizarse a través de "medios de comunicación masiva" entre los que perfectamente pueden incluirse algunos medios que utilizan la informática y nuevas tecnologías ya que muchas de ellas difunden información de manera masiva al gran público. Sin embargo, otras nuevas formas de transmisión de información que pueden utilizar las tecnologías

de la información y comunicación podrían ser excluídas por lo que es necesario efectuar una reforma que contemple cualquier medio de transmisión de información.

4.1.4.3. Exhibiciones o publicaciones obsenas.

> **Artículo 183º.-**
> Será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años el que, en lugar público, realiza exhibiciones, gestos, tocamientos u otra conducta de índole obscena.
> Será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años:
>
> 1. El que muestra, vende o entrega a un menor de dieciocho años, por cualquier medio, objetos, libros, escritos, imágenes, visuales o auditivas, que por su carácter obsceno, pueden afectar gravemente el pudor, excitar prematuramente o pervertir su instinto sexual.
> 2. El que incita a un menor de dieciocho años a la práctica de un acto obsceno o le facilita la entrada a los prostíbulos u otros lugares de corrupción.
> 3. El administrador, vigilante o persona autorizada para controlar un cine u otro espectáculo donde se exhiban representaciones obscenas, que permita ingresar a un menor de dieciocho años.

Sujeto activo

Cualquier persona.

Bien jurídico.

Se protege el poder público y la indemnidad sexual en el caso de la incitación de la práctica de actos obscenos[196].

[196] Bramont Arias y García Cantizano, María. *Manual de Derecho penal*… pp. 277 - 278.

Aspecto objetivo.

En el tipo base se sanciona la conducta de efectuar exhibiciones, gestos o tocamientos de "carácter obsceno" que ofenden al pudor se tienen que realizar en un espacio que se encuentran abiertos o son accesibles a todo el mundo[197]. En este sentido, la exposición en un espacio público implica que el exhibicionista necesariamente debe encontrarse presente en el mismo espacio público.

La conducta descrita en el tipo base se refiere a realizar exhibiciones o conductas obsenas en lugar público. Esta definición restringe la conducta a que se realice únicamente en presencia física de otras personas en un espacio físico, real en el cual entre en contacto (físico) con otros. De esta forma se excluye la exhibición en el ciberespacio o por medios tecnológicos.

Agravante

Se considera una conducta agravada cuando se muestra, pone a la vista o exhibir; entregar o vender con lo cual se proporciona el material de contenido obsceno.

La agravante es dependiente del tipo base por lo que las conductas descritas en el inciso 1 respecto a mostrar, vender, entregar objetos o imágenes de carácter obseno se encuentran enmarcadas en el contexto del espacio físico. En cuanto a la conducta del inciso 2 descrita como "incitar" a un menor a la práctica de un acto obseno puede tambien interpretarse que ésta conducta tiene que realizarse siempre en un espacio físico.

[197] Bramont Arias y García Cantizano, María. *Manual de Derecho penal*… p. 279.

Al respecto, resulta necesario efectuar una reforma legal que sancione conductas que se realicen tanto en un espacio físico como en el ciberespacio ya que la internet y la web cam son utilizadas por pedófilos quienes, ocultandose en el anonimato y la distancia, ofrecen, difunden material obseno o utilizan la tecnología para incitar a menores a practicar actos obsenos.

Objeto material

El inciso 1 indica diversos medios que contienen material obseceno como el libro, objeto, imágenes visuales y auditivas entre los cuales se pueden incluir cualquier soporte que pueda almacenar o reproducir imágenes creados por la tecnología.

4.1.4.4. Pornografía infantil.

> **Artículo 183º A.-**
> El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio incluido la internet, objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de seis años y con ciento veinte a trescientos días multa.
> Cuando el menor tenga menos de catorce años de edad la pena será no menor de seis ni mayor de ocho años y con ciento cincuenta a trescientos sesenta y cinco días multa.
> Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173º, o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil la pena privativa de libertad será no menor de ocho ni mayor de doce años.
> De ser el caso, el agente será inhabilitado conforme al artículo 36º, incisos 1, 2, 4 y 5.

Ciertamente, este artículo responde a la necesidad de establecer una previsión legal que frene el avance de la pornografía infantil.

4.1.6. Contra el patrimonio individual.

Las afectaciones del patrimonio individual no se podían sancionar por los delitos tradicionales que protegían este bien jurídico. Los delitos de hurto encontraban una limitación respecto a la cosa mueble como objeto de apropiación.

En la reforma del Código Penal de 1991 se incluyó en el artículo 186 inciso 3 el delito denominado "hurto telemático o informático" agregando en las modalidades del hurto agravado la sustracción del patrimonio ajeno mediante, a través, o utilizando "sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación de claves secretas".

En el caso de la estafa no puede encuadrarse la conducta de la transferencia de activos o fondos mediante la manipulación de sistemas informáticos con el engaño o error ya que la alteración o manipulación de los datos no se efectúa sobre la persona sino sobre los equipos.

Sin embargo, se debe tener presente que los sistemas informáticos pueden ser utilizados como un nuevo medio para difundir el engaño o las conductas fraudulentas para obtener un provecho económico ilícito. Este es el caso en el cual se ofrecen subastas o se envían cartas para realizar una supuesta inversión o recuperar una fuerte suma de dinero como el caso de la "estafa nigeriana".

4.1.6.1. HURTO AGRAVADO

Especial mención de la agravante por uso de medios informáticos

Artículo 186. 2do párrafo, inciso 3. Hurto informático o telemático

El agente será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años si el hurto es cometido es cometido:

1. En casa habitada.
2. Durante la noche.
3. Mediante destreza, escalamiento, destrucción o rotura de obstáculos.
4. Con ocasión de incendio, inundación, naufragio, calamidad pública o
5. desgracia particular del agraviado.
6. Sobre los bienes muebles que forman el equipaje de viajero.
7. Mediante el concurso de dos o más personas.

La pena será no menor de cuatro ni mayor de ocho años si el hurto es cometido:

1. Por un agente que actúan en calidad de integrante de una organización destinada a perpetrar estos delitos.
2. Sobre bienes de valor científico o que integren el patrimonio cultural de la Nación.
3. **Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o la violación del empleo de claves secretas.**
4. Colocando a la víctima o a su familia en grave situación económica.
5. Con empleo de materiales o artefactos explosivos para la destrucción o rotura de obstáculos.
6. Utilizando el espectro radioeléctrico para la transmisión de señales de telecomunicación ilegales.
7. Sobre bien que constituya único medio de subsistencia o herramienta de trabajo de la víctima.
8. Sobre el vehículo automotor.
9. Sobre bienes que forman parte de la infraestructura o instalaciones de transporte de uso público, de sus equipos o elementos de seguridad, o de prestación de servicios públicos de saneamiento, electricidad, gas o telecomunicaciones.

La primera respuesta del legislador peruano a la criminalidad que utiliza las nuevas tecnologías, aunque limitado a proteger el patrimonio personal, fue introducir el "hurto telemático" o informático en el Código Penal de 1991.

Bien Jurídico del delito de hurto

De acuerdo al Profesor Roy Freyre en el delito de hurto se afecta "directamente contra la posesión e indirectamente contra el derecho de propiedad[198]".

[198] Cfr. Roy Freyre, Luis. *Derecho Penal Delitos contra el Patrimonio*… p.44.

Esta posición es compartida por Bramont Arias Torres y García Cantizano señalan que el bien jurídico tutelado en el delito de hurto es el patrimonio y específicamente la posesión aunque resultara indirectamente lesionado el derecho a la propiedad de la persona[199].

Al respecto Castillo Alva puntualiza que la protección del patrimonio, como todos los bienes tutelados por el derecho penal, se realiza de modo fragmentario[200]. Esto es que la protección penal de este bien jurídico se realiza tipificando acciones concretas.

Elementos objetivos del delito de hurto.

Apoderamiento

El hurto es el tipo base de los delitos de apoderamiento afirma certera y rotundamente Bajo Fernández[201]. En efecto, en los delitos de hurto, robo o apropiación ilícita se procura la incorporación del bien ajeno mediante el apoderamiento que se define como la forma o el modo como el agente incorpora la cosa mueble ajena a su esfera de disposición[202].

Roy Freyre explica claramente que la acción material de apoderamiento se refiere a toda acción de poner bajo su dominio y disposición inmediata un bien que antes se encontraba en la esfera de custodia de otra persona[203]. Esta acción implica "el

---

[199] Bramont Arias Torres / García Cantizano, María. *Manual de Derecho penal*... p. 290. Bajo considera que "la posesión sólo resulta protegida de modo indirecto y como consecuencia de la protección de la propiedad". Por su parte Muñoz Conde siguiendo a Cuello Calón entiende que el bien jurídico es la posesión de hecho de cosas muebles. Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal, Parte Especial* (Delitos patrimoniales y económicos) Ed. Centro de Estudios Ramón Areces. Madrid. 1989.

[200] Castillo Alva, José Luis. Algunas consideraciones sobre el bien jurídico en los delitos contra el patrimonio. En: Revista Peruana de Ciencias Penales. Edición especial sobre el Código Penal peruano. N° 11. p. 213.

[201] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*... p. 21.

[202] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… pp. 45-46, Bramont Arias Torres y García Cantizano, María. Manual de Derecho penal… p. 292.

[203] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 46.

desplazamiento material de la cosa[204]" empero ya no se exige la aprehensión física o material de la cosa debido a que el concepto de objeto material del hurto se ha ampliado a las energías o el espectro electromagnético.

Vives[205] precisa que para lograr el apoderamiento es necesario que el bien se sustraiga del poder de disposición de su propietario el que puede realizarse mediante el ocultamiento.

Bramont Arias Torres, por su parte, subraya que el apoderamiento determina con la "posibilidad inmediata de realizar actos de disposición sobre el bien"[206]. La nota característica del apoderamiento en el hurto es incorporar una cosa ajena a la esfera propia con el ánimo de comportarse como propietario o tener señorío de ésta ya que la posibilidad de disponer del bien ajeno como si fuera propio es también el momento que define la consumación de esta conducta.

Por cierto es de subrayar que el apoderamiento propio del hurto simple o básico debe realizarse sin fuerza sobre las cosas ni intimidación sobre las personas.

En la transferencia electrónica de fondos, el actor no se apodera en el sentido de aprehender o tomar el dinero electrónico o los fondos de forma material, sino que obtiene que una parte de éste salga de la cuenta de la víctima y sea transferido a otra cuenta, obteniendo ya sea el traslado de activos patrimoniales o el pago de servicios o de cuentas. Es una conducta que se puede realizar usando tarjetas de débito, tarjetas bancarias en un cajero o la banca por Internet.

---

[204] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*... p. 32.
[205] Vives Antón. ... p. 328.
[206] Cfr. Bramont Arias Torres y García Cantizano, María. *Manual de Derecho penal*…p. 292

Sustracción

El apoderamiento se encuentra íntimamente vinculado a la sustracción ya que es el medio para lograr el apoderamiento y se define como toda acción para extraer el bien de la esfera de disposición del sujeto pasivo pero es la única forma de obtener el bien[207].

En concordancia con el apoderamiento a través de medios informáticos la sustracción se efectúa sin necesidad de proceder a un desplazamiento físico o material sino que se perfecciona extrayendo, con el uso de la telemática, los fondos que se encuentran en la esfera de disposición que en este caso en particular será la cuenta bancaria o la billetera electrónica que contienen los fondos.

Objeto material

Tradicionalmente los delitos contra el patrimonio individual hurto, robo y apropiaciones tienen a los bienes muebles como objeto material la cosa mueble la cual se ha definido como la cosa "todo aquello que ocupa un lugar en el espacio, es decir, lo que tiene corporeidad, materialidad…"[208] sobre la cual se realizaba una conducta de apoderamiento mediante sustracción. Esta definición ha prevalecido en la doctrina y se considera cosa mueble a todo objeto exterior con valor económico susceptible de apoderamiento material y desplazamiento[209]. Su característica central se encontraba en la corporeidad y movilidad que permiten su apoderamiento mediante la aprehensión y su traslado o incorporación a la esfera de custodia del sujeto activo mediante la sustracción.

---

[207] Cfr. Bramont Arias Torres / García Cantizano, María. *Manual de Derecho penal*…p. 292.

[208] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 49. El concepto es común en la doctrina que hace referencia a "todo objeto material que sea susceptible de apoderamiento capaz de ser transportable y con valor económico." Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal* … p. 36.

[209] Cfr. Muñoz Conde, Francisco; citado por Bramont Arias Torres, Luis y García Cantizano, María. *Manual de Derecho penal*… p. 63 – 64.

El Código Penal de 1924 no definió el concepto de "cosa mueble" y la doctrina nacional excluyó a las cosas incorporales como objeto del delito de hurto[210]. Sin embargo, el Código Penal de 1991 introdujo, en el artículo 185, una definición amplía de cosa mueble acorde con la tecnología, la cual incluye a los bienes incorpóreos que pueden ser desplazados, virtualmente, por medios informáticos.

En el concepto actual de "cosa mueble" comprende elementos que tengan valor económico, entre los cuales se encuentran las energías; la luz y el gas; el agua, el espectro electromagnético que son las ondas de radiofrecuencia generados por dispositivos electrónicos[211]. Adicionalmente, en el concepto de "cosa mueble" se incluyen los fondos o dinero electrónico como objeto específico del hurto telemático. Con esta fórmula legal la información que represente parte de los activos patrimoniales o el denominado "dinero electrónico" pueden ser, a través de transferencias no consentidas de fondos, objeto de desplazamiento y apoderamiento ya que éstas son extraídas de una cuenta y son transferidas a otras.

La definición de cosa mueble ampliada por el artículo 185 para superar las limitaciones propias de los objetos corpóreos permite adecuar la norma penal a fin de cautelar eficientemente el patrimonio individual. En efecto, en tiempos actuales los bienes incorpóreos representan al patrimonio como en el caso del dinero contable que se encuentra representado en datos informáticos o las energías. Sin embargo, el vocablo "elemento" como sinónimo de cosa no resulta adecuada pues significa, de acuerdo al Diccionario de la RAE, componente o parte integrante de algo mientras que cosa es todo aquello que tiene que tiene entidad, corporal o espiritual, u objeto inanimado. Se pudo definir el concepto indicando "se equipara

---

[210] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 51.

[211] Cfr. Bramont Arias Torres y García Cantizano, María. Manual de Derecho penal… p. 293. En la modificación realizada mediante el Decreto Legislativo Nº 1084 se incluyó en el concepto de cosa mueble los límites de captura de pesca. Por su parte, Rojas Vargas sostiene que "Ha de tratarse de un mueble, esto es, una cosa que sea extraíble y trasnportable." Rojas Vargas, Fidel. *Delitos contra el patrimonio*. Vol I. Grijley. Lima 2000, p. 132.

a bien mueble cualquier tipo de energía, el agua, el espectro electromagnético, los recursos pesqueros superiores a los límites máximos de captura por embarcación o cualquier otra cosa, material o inmaterial, con valor económico."

Con el nuevo concepto o el concepto funcional de cosa mueble que trae el Código Penal de 1991 ya no es necesario acreditar un apoderamiento material constatable ex post[212] para que la conducta se consume ya que en muchos casos el dinero electrónicamente transferido se queda en las cuentas o se transfiere de una a otra cuenta para que se pierda el rastro de la operación.

La información con valor económico[213] pueden ser el objeto material tal como ha sido interpretado en la jurisprudencia[214]. Este concepto comprende a cualquier dato que tenga valor económico que puede ser sustraído de una base de datos procesada informáticamente.

La cosa o el bien mueble, para que sea apta para ser el objeto material en el sentido que expresa el artículo 185 del Código Penal, especialmente en el denominado "hurto telemático" en la transferencia electrónica de fondos son, precisamente, los

---

[212] Cfr. Reyna Alfaro, Luis Miguel. *Los delitos informáticos*… p. 327. Rojas Vargas, Fidel. *Delitos contra el patrimonio*… p.133, por su parte, entiende que "el concepto de bien mueble ampliado y enriquecido con otros componentes provenientes, unos de los bienes inmuebles, como el agua, o de otros contextos no de otros contextos no expresamente regulados en el código civil, como es el caso de la energía eléctrica, el espacio electromágnetico y los gases. Pero esta asimilación debe ser conciliada en lo mínimo con el principio de aprehensibilidad que domina la naturaleza desplazable o movilizable del bien mueble." Sin embargo, el apoderamiento por medios informáticos se refiere al desplazamiento y apoderamiento virtual mediante el cual se ingresa el bien a la esfera de disposición del agente. El "apoderamiento virtual" que se puede realizar mediante la tecnología no encaja en el concepto tradicional de aprehensión entendida como agarrar, sujetar o aferrarse a una cosa. Lo mismo ocurre con el apoderamiento de agua o energías en el cual se produce al desviar el curso del agua, mediante un canal o tuberías, o conectando cables a una caja de luz. En el apoderamiento del espectro electromagnético tampoco se puede exigir el "mínimo de aprehensibilidad" pues se trata de ondas de radio utilizadas en la radio difusión. En rigor, se trata más bien de la desmaterialización del concepto de bienes o cosas muebles para permitir incluir a objetos inmateriales sobre los cuales no puede concebirse el apoderamiento de manera tradicional.

[213] Cfr. García Cantizano, María. *La delincuencia informática en el ordenamiento jurídico peruano*. En: Gaceta Jurídica. Tomo 78-B, Mayo 2000, p. 70.

[214] Ejecutoria Superior de la Sala Penal de Apelaciones para procesos sumarios de la Corte Superior de Lima (EXP. 4177-98) de fecha 16 de noviembre de 1998, donde se decidió un hurto de información computarizada en agravio de la empresa Diners Club Perú SA, En Rojas, p. 284.

fondos entendido como activos o dinero electrónico, pero cuando la norma penal se refiere ampliamente al uso de la telemática, se trata de cualquier elemento informático con valor económico y que forma parte del patrimonio individual[215].

El valor económico del bien objeto del delito de hurto se encuentra precisado por la ley penal en el artículo 444 del Código Penal; esto es superior a 4 RMV. Si las conductas de sustracción o apoderamiento sin violencia recaen sobre cosas con un valor inferior serán consideradas faltas.

De acuerdo con el Código Penal el hurto, esto es la sustracción y apoderamiento de una cosa mueble ajena, se agrava cuando se realiza, entre otras circunstancias:

> 3. Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o la violación del empleo de claves secretas.

El segundo párrafo del artículo 185 contiene, en el inciso 3, dos modalidades agravadas de hurto; i) el hurto telemático y ii) el hurto por violación de claves secretas. Esta agravante, como todas las modalidades agravadas, dependen del tipo base[216] donde se describe la conducta punible y en la agravante se agrega una condición, circunstancia o modalidad comisiva que califican la conducta básica. Se trata pues de un hurto, es decir, apoderamiento mediante sustracción, calificado por la transferencia electrónica no consentida de fondos.

Como se sabe, las agravantes son circunstancias que incrementan el injusto de la conducta del tipo base, por lo que el elemento objetivo del delito de hurto telemático son el apoderamiento y la sustracción. En este caso, esta agravante se

[215] Cfr. Rojas Vargas, Fidel. *Delitos contra el patrimonio*… p. 284.
[216] Cfr. Rojas Vargas, Fidel. *Delitos contra el patrimonio*… p.170.

califica cuando esa conducta utiliza como medio comisivo la telemática o cuando se violan las claves secretas.

Las modalidades señaladas en el artículo 186 se refieren a circunstancias concretas que aumentan el disvalor[217] del hurto que se refieren a circunstancias concretas de apoderamiento de cosa mueble ajena mediante sustracción utilizando elementos informáticos como la telemática o con violación de claves secretas.

La solución peruana, tipificada en 1991, de sancionar las frecuentes afectaciones del patrimonio individual cometidas por medios informáticos, fue tipificarlas en como una forma agravada del hurto para ello se tuvo que ampliar el concepto de cosa mueble a energías o "elementos" con valor económico. Sin embargo, como bien dice Mazuelos[218] "toda la problemática de la delincuencia informática no puede ser abarcada por el precepto en análisis, el delito de hurto comprendería únicamente las afectaciones al patrimonio bajo las modalidades allí descritas".

Las conductas de apoderamiento y sustracción de cosas ajenas son perfectamente aptas para encuadrar el hurto por medio de elementos electrónicos; sin embargo, el legislador ha encontrado un mayor disvalor de la acción en estas conductas por la mayor dañosidad del medio empleado y las ha ubicado en el tipo agravado.

El principio de legalidad nos obliga a aplicar todas las características del tipo básico a los supuestos del tipo agravado[219] aunque Fidel Rojas[220] no comparte este criterio y entiende que la modalidad agravada interesa más la modalidad que el

[217] Cfr. García Cantizano, María. *La delincuencia informática en el ordenamiento jurídico peruano*… p.70, explica que la agravante se encuentra justificada en función al medio empleado por el sujeto activo del delito.
[218] Cfr. Mazuelos, Julio. *Delitos informáticos*… p. 294
[219] Cfr. Castillo Alva, José Luis. *Algunas consideraciones sobre el bien jurídico en los delitos contra el patrimonio*… p. 228.
[220] Cfr. Rojas Vargas, Fidel. *Delitos contra el patrimonio*... p. 172.

valor del bien y "lo que no puede ser hurto simple si puede ser hurto agravado" (sic).

Felizmente, Castillo Alva nos da la "interpretación correcta"[221] al respecto e insiste que -en el hurto agravado- se exige la concurrencia de todos los elementos del hurto simple[222].

i) hurto telemático.

La telemática es la unión de las comunicaciones con la informática que permite el envío de cualquier tipo de datos a través de las redes informáticas. Etimológicamente proviene de dos palabras griegas *tele* (distancia o lejos) y *mática* (ciencia o artificio)[223]. Hay que tener en cuenta que en términos informáticos la expresión data[224] se refiere a cualquier clase de información almacenada en forma de bytes en una memoria electrónica por lo que este término comprende tanto a la información bancaria o de las cuentas personales como a cualquier otro archivo que represente activos patrimoniales o no.

La transferencia electrónica de fondos es el traslado de dinero de una cuenta bancaria a otra o el movimiento de información con respaldo dinerario[225]. A través de la transferencia electrónica de fondos (TEF) se puede mover dinero entre cuentas, el pago de servicios o efectuar el pago mediante tarjetas de crédito o débito. Lo singular de estas transferencias es que no existe intercambio de dinero en metálico, en efectivo o mediante títulos valores pues lo único que se envía es información que contiene los datos respecto a las cuentas bancarias.

---

[221] Cfr. Castillo Alva, José Luis. *Algunas consideraciones sobre el bien jurídico en los delitos contra el patrimonio*... p. 228.
[222] En rigor esta regla es aplicable cuando el código establece circunstancias agravantes de conductas como el asesinato o el parricidio que se asientan sobre el delito de homicidio o en el caso de las agravantes del artículo 297 que se construyen sobre el tipo base del tráfico ilícito de drogas artículo 296.
[223] Vide: http://es.wikipedia.org/org/wiki/Telemática
[224] Vide: http://www.webopedia.com/TERM/data.html
[225] Cfr. Bramont Arias y García Cantizano, María. *Manual de Derecho penal*… p. 302.

Mediante la telemática se realiza la transferencia electrónica de fondos en la cual un cliente solicita en un establecimiento del abono de una compra o el pago de servicios, (luz, agua, teléfono, etc) mediante una terminal (POS) que autoriza que se pague la operación con el saldo de sus cuentas bancarias (en el caso de usar una tarjeta de débito) o la línea de crédito autorizado (cuando se utilice una tarjeta de crédito). La telemática también es el medio para transferir dinero electrónico para efectuar pagos.

La telemática o la informática a distancia[226] es una de las características más notorias de los sistemas informáticos es su conectividad o vinculación entre computadoras. Las comunicaciones entre computadoras se logra a través de la telemática y la transferencia electrónica de fondos es una de las formas de utilizar la telemática.

La conducta típica se refiere a la sustracción y apoderamiento del dinero electrónico[227] que se encuentra en una cuenta bancaria mediante el uso de una medio de pago electrónico. El uso indebido de tarjetas de crédito mediante el cual se obtiene el pago de servicios no se incluye en el supuesto de hurto telemático, pues en ese caso no se efectúa una transferencia de fondos o dinero contable sino que se obtiene la autorización del uso de una línea de crédito. En este caso no existe apoderamiento ni sustracción de cosa mueble, pues el agente no realiza una transferencia electrónica de fondos o de dinero electrónico sino que obtiene indebidamente un crédito.

---

[226] Cfr. García Cantizano, María del Carmen. *La delincuencia informática*... p. 70.

[227] El Código penal peruano se refiere exclusivamente a "fondos" el cual debe interpretarse como dinero o los caudales en efectivo. Además, las transferencias electrónicas de fondos están referidas únicamente al dinero electrónico. El dinero electrónico es aquel creado, cambiado y gastado de forma electrónica. Este dinero tiene un equivalente directo en el mundo real: la moneda. Cfr. Mazuelos, Julio. *Delitos informáticos*… p. 295. http://es.wikipedia.org/wiki/Sistema_de_pago_electrónico

Respecto al hurto de información,[228] para que se incluya como objeto material del hurto telemático, la información o data deberá tener valor económico y formar parte del patrimonio para que su apoderamiento ocasione un perjuicio económico. Sobre este punto, Mazuelos[229] sostiene que "la información procesada, desde luego, no sería abarcada por esta modalidad de hurto en la medida que no se trataría de un bien mueble ni siempre puede ser apreciada en términos económicos, lo cual dificultaría su comprensión como un delito contra el patrimonio."

El código penal se refiere a energías u otro elemento con valor económico de manera genérica no se circunscribe únicamente a la energía sino que amplía el objeto material a otras cosas además de las energías. De acuerdo a esta interpretación se puede incorporar como objeto material a cualquier otro elemento electrónico con valor económico siempre que su apropiación se efectúe utilizando la telemática.

ii) **Violación de claves secretas.**

De acuerdo a Bramont Arias Torres esta modalidad está referida al uso indebido de las claves en los cajeros automáticos[230].

La modalidad de "violación de claves secretas" puede estar referida tanto al acceso a sistemas informático como a la apertura de otros sistemas de seguridad no informáticos[231] ya que las "claves secretas" son todas las contraseñas (passwords) o los códigos de seguridad para abrir cualquier sistema de seguridad. Esto es, que el agente se apodere del patrimonio ajeno manipulando los terminales de cajeros automáticos o los terminales de puntos de venta (POS) a los cuales accede violando

[228] Cfr. Bramont Arias y García Cantizano, María. *Manual de Derecho penal*.. p. 302.
[229] Cfr. Mazuelos, Julios. *Delitos informáticos…* p. 295.
[230] Cfr. Bramont Arias y García Cantizano. *Manual de Derecho penal*… p. 302.
[231] Cfr. Mazuelos, Julio. *Delitos informáticos*... p. 296. Bramont Arias T., Luis, *El delito Informático en el Código Penal Peruano*… p. 71

las claves secretas del usuario. No obstante, esas conductas se encuentran incorporados en el supuesto del hurto telemático ya que en ambos casos, además de emplear "claves secretas", se utiliza la telemática para apoderarse del patrimonio ajeno.

Por ello, Mazuelos[232] ha resaltado la "insatisfactoria redacción" de este precepto ya que no establece diferencia entre la forma de obtener la clave o el uso indebido de quien la conoce por alguna causa lícita o por autorización del titular de la cuenta.

No considero que se deba incorporar en esta modalidad los procesos de encriptado de textos como propone Rojas[233]. El encriptado o cifrado de textos o documentos es una medida de seguridad que permite, mediante fórmulas matemáticas, ocultar o disfrazar su contenido evitando que este sea conocido por terceros. El receptor de la comunicación para descifrar el mensaje debe utilizar su clave del descifrado. Sin embargo, la violación o el uso indebido de la clave de descifrado no es un medio para apoderarse o sustraer un bien ajeno sino que el agente únicamente consigue el acceso a la información, pero no se apodera de ella, en el sentido que tiene esta conducta en el hurto, el cual es incorporar un bien ajeno a su patrimonio. Por esta razón considero quela tesis de Rojas Vargas no encuentra sustento.

Consumación

Como ocurre en el hurto, en esta modalidad agravada se consuma cuando se produce el apoderamiento; es decir, cuando el sujeto activo tiene la disponibilidad[234]. Se admite la tentativa.

---

[232] Cfr. Mazuelos, Julio. *Delitos informáticos...* p. 296.
[233] Cfr. Rojas Vargas, Fidel. *Los delitos contra el patrimonio…* p. 286.
[234] Cfr. Bramont Arias y García Cantizano, María. *Manual de Derecho penal…* p. 295. Respecto al tipo base subrayan que únicamente se requiere "una mínima disponibilidad".

En el caso de la transferencia electrónica de fondos se puede establecer que el agente tiene la disponibilidad de los fondos ajenos cuando éstos se encuentran en la cuenta del agente o de un tercero.

Concurso

Existiría un concurso aparente de leyes entre la conducta prevista en el artículo 186 inciso 3 y el segundo párrafo del artículo 207- A ya que el acceso indebido puede servir para realizar transferencias de fondos de una cuenta a otra. Este concurso se debe resolver aplicando el principio de subsunción[235]. El uso de claves secretas, para Mazuelos[236], se encuentra prevista en la Ley de Delitos Informáticos.

Sin embargo, hay que tener en cuenta que el artículo 207-A se refiere a "beneficio económico" el cual es un concepto más amplio que el objeto material del hurto telemático en el cual se restringe al apoderamiento a dinero electrónico.

4.1.6.2. HURTO DE USO[237].

> **Artículo 187.-** El que sustrae un bien mueble ajeno con el fin de hacer uso momentáneo y lo devuelve será reprimido con pena privativa de libertad no mayor de un año.

Bien Jurídico.

Concretamente es la posesión. El derecho del propietario de utilizar y disfrutar la cosa como derecho derivado de la propiedad o el derecho del poseedor legítimo de usar el bien.

---

[235] Cfr. Bramont Arias Torres, Luis. *El delito informático*… p. 74. Para Mazuelos, Julio; de acuerdo al principio de especialidad "resulta actualmente de aplicación lo establecido en el artículo 207-A, segundo párrafo, máxime si el inc. 3 del artículo 186, segundo párrafo, no hace alusión expresa al empleo de una computadora o sistema informático". Cfr. *Delitos informáticos*… p. 295.

[236] Cfr. Mazuelos, Julio. *Delitos informáticos*... p. 297.

[237] Vide: propuesta legislativa peruana sobre el hurto de tiempo.

Elementos objetivos

Sujeto activo.

Cualquier persona excepto el propietario o el condómino.

Sujeto pasivo.

Cualquier persona que poseía el bien.

Sustracción. Se refiere siempre a extraer el bien fuera de la esfera de vigilancia del sujeto pasivo pero en este caso, a diferencia del hurto simple, la sustracción es el único elemento comisivo el cual, además tiene un fin específico: utilizar la cosa por un periodo corto de tiempo.

Se trata pues de un desplazamiento o la extracción temporal fuera de la esfera de vigilancia del sujeto pasivo, por ello en esta conducta no existe el apoderamiento. En rigor, la cosa no ingresa a la esfera de disposición del agente en el sentido del delito de hurto tipo base.

Devolución. Se refiere a la restitución de la cosa a la esfera de vigilancia aunque no se trata de una entrega al sujeto pasivo sino que es suficiente con ponerla a su alcance. Solo podrá hablarse de "devolución" si el agente activamente haya participado en la devolución del bien.

Uso momentáneo.

Seguramente el legislador pretendió indicar, con este impreciso elemento normativo, que el uso durara más de unas horas.

Objeto material.

El objeto o el bien mueble debe reunir tres características: i) ser una cosa mueble corpórea, ii) ser totalmente ajena y iii) no consumirse con el uso. Entonces, la

cuestión aquí es determinar si el concepto del bien mueble que contiene el artículo 185 resulta aplicable a esta conducta. Me inclino a pensar que no porque el objeto que se toma debe ser capaz de regresar a la esfera de disposición del sujeto pasivo básicamente en las mismas condiciones en las que se encontraba cuando fue sustraído sin consumirse con su uso. En el caso de las energías, la luz o el gas, o el agua las cuales por su propia naturaleza se consumen o agotan con su uso y no hay manera de restituirlas en el mismo estado en el que se sustrajo. En realidad esta es una conducta importada[238], parafraseando a Hurtado Pozo, de la legislación española que sancionaba la sustracción de vehículos para un uso momentáneo o temporal.

Aspecto sujetivo.

Dolo directo. Conocimiento que se sustrae una cosa ajena. En este caso, no hay ánimo de lucro en el sentido de aprovecharse del valor de la cosa. Bajo Fernández[239] encuentra que la distinción central entre el hurto común y el hurto de uso estriba que en este no existe "ánimo de hacerla como propia".

4.1.6.3 Estafa.

El tipo penal de estafa se construye sobre los siguientes elementos: i) engaño u otra forma fraudulenta, ii) error, y iii) perjuicio patrimonial.

> **Artículo 196.-** El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años.

[238] El Código Penal Español tipifica la conducta de "hurto de uso de vehículos" por la alta tasa de sustracciones de vehículos para realizar cortos paseos o darle un uso concreto al vehículo. Conducta que no se realiza en nuestro país. Por cierto, el tipo en referencia al controversial e impreciso "uso momentáneo" sino que establece un plazo de 48 horas.

[239] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*… p. 27.

Sujeto activo.

Puede ser cualquier persona.

Sujeto pasivo.

Se trata del títular del patrimonio afectado[240]. Puede ser cualquier persona incluso otra distinta a la engañada que incurrió en error como sucede en la "estafa en triangulo"[241]; sin embargo, son la misma persona el sujeto pasivo y el perjudicado[242].

Por lo tanto, no es necesario que el engañado y el perjudicado sean la misma persona[243].

Bien jurídico

En la doctrina se considera, de manera unánime, al patrimonio como el bien jurídico protegido en las defraudaciones[244]. En la estafa se protege, concretamente, la situación de disposición que tiene un sujeto sobre bienes, derechos o cualquier otro objeto[245].

Muñoz Conde[246] precisa que se trata de cualquier elemento del patrimonio ajeno, bienes muebles, inmuebles, derecho y al mismo tiempo se lesiona la buena fe o las relaciones fiduciarias que surgen del tráfico jurídico.

---

[240] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*… p.165.
[241] Cfr. Bramont Arias Torres / García Cantizano, María. Manual de Derecho penal… p. 349.
[242] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*… p. 174.
[243] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*… p. 174.

[244] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*… p.164.
[245] Cfr. Bramont Arias y García Cantizano, *Manual de Derecho penal*… pp. 345-346.
[246] Cfr. Muñoz Conde, Francisco. *Derecho Penal*… p.295.

Existen tres posiciones sobre el concepto de patrimonio[247]; a) concepcion juridica del patrimonio que considera al patrimonio "el conjunto de derechos patrimoniales de una persona; b) Concepcion economica del patrimonio en el cual es el conjunto de bienes que se encuentran bajo el poder de disposicion de una persona y c) Concepcion mixta o juridico-economica del patrimonio que comprende a todas las cosas con valor economico que revisten una apariencia juridica.

El Código Penal peruano sigue el sistema genérico de la estafa[248] consignando los elementos constitutivos: engaño (medio comisivo); error (suscitado o mantenido en la víctima); provecho económico ilícito (propósito perseguido u obtenido por el agente); y, perjuicio patrimonial (resultado contra la víctima)

En conclusión, se protege la disposición de cualquier elemento integrante del patrimonio individual.

Aspecto objetivo.

El delito de estafa es una obra en tres actos que se construye sobre el engaño, error y perjuicio patrimonial. Estos elementos se encuentran concadenados y aparecen secuencialmente concadenados a partir del engaño generado o creado por el agente. A partir de éste los otros caen como en efecto dominó. En efecto, como veremos a continuación, el engaño genera el error y éste, a su vez, ocasiona el perjuicio patrimonial. Por ello, el engaño o sus equivalentes es una condición "cuantitativamente dominante[249]" anterior al acto de disposición y se establece una relación de causalidad ideal o de motivación: el engaño ha de motivar (producir) un error que induzca a realizar un acto de disposición que determine un perjuicio. Han de hallarse exactamente en la relación consecuencial descrita por la ley[250].

[247] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*… p. 166.
[248] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*... p. 148
[249] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*... p.170.
[250] Vives 401.

De acuerdo a la descripción típica de la estafa, el agente accede al patrimonio ajeno no mediante la sustracción sino mediante el "engaño, astucia, ardid u otra forma fraudulenta". Roy Freyre[251] describe la estafa de manera pedagógica. El estafador alarga la mano, no para coger las cosas, como ocurre con el ladrón, sino para que la víctima se las ponga a su alcance.

En la estafa, en el cual el sujeto activo procura con una actividad fraudulenta que el sujeto pasivo coloque el bien en su esfera de disposición, existe una relacion de causalidad[252] entre el engaño que produce el error el cual a su vez induce la disposicion patrimonial.

1. **Engaño u otra forma fraudulenta.**

   Aunque el tipo penal describa los elementos normativos como "engaño, astucia, ardid u otra forma fraudulenta" la conducta central es el engaño ya que este concepto comprende a los otros pues significan acciones contrarias a la verdad en perjuicio de otro. Por lo tanto, engaño u otra conducta fraudulenta es cualquier enmascaramiento, simulación o disfraz de la verdad capaz de hacer incurrir en error a otra persona.

   El engaño es además, el primer y "más significativo"[253] elemento de la estafa y la individualiza frente a las otros delitos contra el patrimonio pues las conductas de hurto, robo o apoderamiento se realizan mediante el apoderamiento.

[251] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 154.
[252] Vives 401.
[253] Vives p. 401

El engaño u otra forma similar de disfrazar la verdad es elemento central de la estafa el cual, en palabras de Roy Freyre[254], es simulación o disimulación de sucesos y situaciones de hecho, materiales o psicológicos con las que se logra que caiga la persona en error.

Roy Freyre[255] indica que el engaño necesita elementos externos -*mise en scene*- para poder dar verosimilitud a la afirmacion fraudulenta del agente. Esta teoría explica la exigencia de un medio artificioso para la configuración de la estafa. El estafador debe utilizar medios externos que le proporcionan mayor valor o hacen verosímil su afirmación o la propuesta fraudulenta como cuando se muestra documentos falsos para acreditar la propiedad de un inmueble. De esta manera, el uso de la *mise en scene* que implica que se requiera más que una simple mentira, que un simple silencio o un puro juicio valorativo[256].

En la doctrina penal se hace referencia a la idoneidad del engaño para lo cual se debe tener en cuenta no solo la actividad desplegada por el agente sino, fundamentalmente, las condiciones personales de la víctima. Esto es, sus condiciones y circunstancias personales como edad, educación. Por ello, que se deberá adoptar un criterio objetivo - subjetivo[257], en el cual se debe tomar en cuenta, por un lado, si el engaño es capaz de vencer la diligencia y cuidado de la víctima y verificar las condiciones personales del sujeto pasivo para deteminar en cada caso en particular el engaño[258].

---

[254] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*... p.156.
[255] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*... p.154.
[256] Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal*... p. 169.
[257] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 164. Bramont Arias Torres / García Cantizano, María. *Manual de Derecho penal*… p. 349
[258] Cfr. Bustos Ramírez, Juan. *Manual de Derecho penal*... p. 191. Entiende que "habrá de considerar la manifestación o la imagen falsa en relación al sujeto concreto y en cada caso particular conforma a sus circunstancias precisas."

2. **Error**.

Este segundo elemento es la bisagra entre el engaño y la disposición patrimonial. El engaño produce o genera error o el "conocimiento viciado de la realidad"[259] y además ocasiona el perjuicio patrimonial. Me refiero aquí que se exige extrictamente un "engaño a otro". Esto es, la víctima va a disponer o entregar parte de su patrimonio en base a tener una visión distorsionada de la realidad o, como se puede decir, cuándo ha sido engañado. Se trata de un concepto equivocado o juicio falso o distinto de la realidad que tiene una persona ocasionado por la conducta fraudulenta desplegada por el agente y a partir de éste se produce la entrega de parte del patrimonio.

Mayoritariamente en la doctrina se considera al error como un estado psicológico, pues constituye un efecto mental[260] por ello únicamente las personas físicas pueden incurrir en él.

El tipo penal establece que la conducta del agente debe "*inducir o mantener a error*" a la víctima, con lo cual es posible que éste esté en error con anterioridad. En este supuesto, la conducta del agente está dirigida a reafirmar o corroborar la falsa apreciación que tiene la potencial víctima. Sin embargo, no se trata del puro silencio sino que debe desplegar una conducta positiva y activa o que exista un deber jurídico de hablar o decir la verdad.

En consecuencia, "*mantener en error*" únicamente tiene relevancia penal cuando fortifica o impide el cese del error mediante el engaño[261].

---

[259] Cfr. Bajo Fernandez, Miguel y Pérez Manzano, Margarita. Aspectos generales del tipo de estafa, Donna, Alberto y Javier E. De la Fuente p. 70.
[260] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 157. García Cantizano, María. *La delincuencia informática*… p. 71. Vives p.405
[261] Cfr. Bramont Arias Torres / García Cantizano, María. *Manual de Derecho penal*… p. 350.

3. Perjuicio patrimonial

Perjuicio patrimonial es la disminución del conjunto de los valores económicos de una persona, entendido como la pérdida de una parte de éste o una disminución económica del patrimonio en su conjunto[262] a consecuencia del error inducido mediante engaño[263].

Se trata de una pérdida valuable económicamente, siempre a consecuencia del engaño, a partir de la entrega o puesta a disposición del agente de parte del patrimonio. Por lo tanto, se exige que se materialice la pérdida o disminución del patrimonio por ello si el agente realiza una compensación entregando otro bien de un valor similar al ofrecido no existe estafa por que se elimina el perjuicio[264].

El perjuicio se produce con **el acto de disposición[265]** es decir, con la entrega voluntaria o *traditio* de parte del patrimonio al agente aunque con la voluntad viciada por el engaño pues se realiza en la creencia que esta entregando parte de su patrimonio en contraprestación de un bien o servicio ofrecido.

Para que exista un "acto de disposición" no es necesario una entrega física o personal del bien sino que es suficiente con ponerla a disposición del agente

---

[262] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 169.
[263] Vives p. 410.
[264] Cfr. Bramont Arias Torres / García Cantizano, María. *Manual de Derecho penal…* p. 354. Es de subrayar que no existirá estafa aunque exista engaño pero no se verifica el perjuicio patrimonial como cuando ocurre si el agente entrega algo de valor similar. Bajo Fernández explica que "Hay compensación solo cuando la pérdida de la cosa (o valor económico) se compense con otro valor económico. Así por ejemplo, no hay delito de estafa, por inexistencia de perjuicio, si se vende un cuadro de Zurbarán afirmando es de Murillo, cuando se vende al precio justo del mercado. Cfr. Bajo Fernández, Miguel. *Manual de Derecho Penal…* p. 174. En el mismo sentido, Vives señala que "Si la contraprestación que se recibe es de igual valor que la que se realiza no hay delito" Ob. Cit. p. 410. Vives adopta el concepto económico jurídico del patrimonio. Vives… p. 316.
[265] Extensamente sobre el "acto de disposición" Bramont Arias Torres / García Cantizano, María. Manual de Derecho penal… p. 352.

como sería el caso que la víctima disponga la entrega de bienes del almacén o por sus dependientes[266].

La "estafa en triángulo" se produce cuando una persona dispone de un bien perteneciente a un tercero. En este supuesto, la persona engañada entrega o pone a disposición del bien. Este sería el caso en el cual el agente utilice una tarjeta de crédito ajena o adulterada para efectuar compras y presenta la tarjeta a la cajera, quien entrega el bien a éste.

Objeto material.

El objeto material de la estafa o la cosa que se entrega a consecuencia del engaño es cualquier elemento integrante del patrimonio sea mueble o inmueble. También se incluyen los fondos o el dinero electrónico y la información digitalizada con valor económico.

Consumación.

Se trata de un delito de resultado, por lo tanto la estafa se perfecciona con el perjuicio patrimonial. Si no se llega a producir la disminución el patrimonio estaríamos frente a una tentativa.

4.1.6.3.1. Estafa por medios informáticos.

Como hemos visto, una de las primeras conductas cometidos contra el patrimonio individual con el uso de la informática se denominó "computer fraud" o fraude por computadoras aunque era un término que no se subsumía en el tipo penal de

[266] Una modalidad típica de estafa es la realizada con la compra de bienes a empresas a las cuales se les engaña a los encargados de la venta con la presentación de un cheque falsificado de otra persona con el cual cancelan la compra y los empleados de la empresa vendedora autorizan la entrega de los bienes del almacén.

estafa. Simplemente se designó con ese nombre a las conductas que ocasionaban un perjuicio patrimonial.

Es de mencionar que en la descripción típica del engaño -en el sentido clásico en la cual se requiere una relación directa y personal entre dos seres humanos- que genera perjuicio patrimonial, no se subsume a las manipulaciones o alteraciones del sistema informático.

En efecto, se exige que el engaño o la conducta fraudulenta sea "idónea" o "suficiente" para inducir a error a la víctima. De acuerdo a esta definición, las máquinas no pueden ser sujetos pasivos de la estafa ya que no pueden ser "engañadas" como a un ser humano ni incurrir en error pues como bien nos dice Gutierrez Frances el ordenador sólo podrá ser objeto o instrumento no víctima o sujeto de acción.[267]

Entonces, si no hay error de acuerdo a su concepción psicológica que exige el estado mental de la víctima quien tiene una falsa representación mental de la realidad que origina la disposición patrimonial (requisito necesario para la configuración del tipo), no hay estafa.

Desde esta perspectiva, el tipo clásico de estafa no puede, por la limitación del principio de legalidad, subsumirse a las conductas que manipulan los datos de un sistema informático o cajeros automáticos para obtener un beneficio económico. Sin embargo, el uso de tarjetas ajenas (robadas o no) o tarjetas clonadas pueden equipararse a la conducta de engañar y hacer incurrir en error que se exige en la estafa cuando estas conductas se ejercercen sobre una persona física conforme ha sido precisado en la jurisprudencia:

[267] Cfr. Gutiérrez Francés, María Luz. *Delincuencia Económica e informática en el Nuevo Código Penal...* p.268.

> Que, para la configuración del delito de estafa, se requiere del engaño, error, depreciación patrimonial, perjuicio (tipicidad objetiva); dolo y ánimo de lucro (tipicidad subjetiva). Que en el presente caso, en la conducta desplegada de la acusada existe un engaño, pues a sabiendas de que la tarjeta de crédito no le pertenecía, hizo uso de ella como si fuere la titular, generando por parte de los agraviados una disposición patrimonial. Exp. Nº 8721-97-Lima[268].

En conclusión, cuando la acción del sujeto activo se ejecute sobre la máquina o sistema informático, esta conducta no se podrá adecuar al tipo penal clásico de estafa y, por este motivo, en los códigos penales español y alemán se introdujo una reforma que incluyen las "manipulación informática o artificio semejante" que alteren el procesamiento de datos para obtener un beneficio económico. En el caso de las manipulaciones informáticas el agente ingresa un código distinto al suyo, o altera sus rutinas para obtener un beneficio patrimonial nunca existe el contacto humano y por ello ni se despliega una conducta engañosa o fraudulenta ni la máquina incurre en error entendido como un estado psicológico de la vícitma producto de la conducta fraudulenta del agente[269].

De acuerdo a lo expuesto, extraer dinero de un cajero automático o una terminal con una tarjeta clonada o robada no se puede considerar estafa porque no se puede engañar a una máquina, sino que se trata de una transferencia no autorizada de fondos sancionada en el Código Penal peruano como hurto agravado en la modalidad de hurto telemático.

Debido a que la lesión del patrimonio ajeno utilizando la computadora no puede subsumirse en el tipo penal de estafa clásica o genérica, debido a que la alteración o modificación de la rutina de los programas para obtener un beneficio patrimonial no puede equipararse al engaño ni puede considerarse que la máquina que efectúa

[268] En: *Actualidad Jurídica*. Tomo 141. agosto de 2005. p. 111.

[269] Donna, Ob cit. p. 68.

la disposición patrimonial no puede interpretarse que ha incurrido en error, las legislaciones españolas y alemanas han efectuado una tipificación especifica para esta nueva conducta.

El delito de estafa tipificado en el código penal español, por medios informáticos, tiene como elemento central las "manipulación informática o artificio semejante" que produzca la transferencia de un activo patrimonial se entienden como "una alteración o modificación de datos[270]" De acuerdo a Gutierrez Frances, esta previsión legal sólo sirve para combatir ataques al patrimonio como bien jurídico de carácter individual microsocial,[271] ya que aunque el concepto "activo patrimonial" comprende cualquier elemento que integre el patrimonio individual sin la limitación del objeto material; esto es si es cosa mueble o inmueble, encuentra su límite en el bien jurídico el cual está referido a la tutela del patrimonio individual.

La nueva estafa informática es "toda manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en cualquier momento de éste, realizada con ánimo de lucro y causando perjuicio económico a un tercero." De otro lado, la cláusula abierta "artificio semejante" se entiende como "toda manipulación operada sobre ficheros o soportes informáticos, electrónicos o telemáticos[272]" en la cual ya no se exige la "inmediatez" entre dos seres humanos.

En la manipulación informática como objeto del engaño, es necesaria que dicha maniobra sea captada, percibida física o visualmente por una persona, una captación del contenido de los datos manipulados, de forma que, como consecuencia de

[270] Vives p. 414.
[271] Cfr. Gutiérrez Francés, María Luz. Los fraudes informáticos en el nuevo Código Penal. En: Los delitos relativos a la informática. En: El Código Penal de 1995: Parte especial. Consejo General del Poder Judicial. Barcelona, p.255.
[272] Vives p. 415.

la misma, se modifique su representación intelectual sobre la realidad que ha sido falseada.[273]

Las manipulaciones informáticas con ánimo de lucro se realizan "dentro del sistema" y "fuera del sistema". Esta clasificación, únicamente por fines pedagógicos, se refiere a la forma de efectuar la infiltración del sistema informático. Las primeras la alteración se efectúa directamente sobre el sistema operativo y, las segundas, se realizan antes, durante o después de la elaboración del programa[274].

En la nueva conducta de estafas informáticas el acto de disposición y su consiguiente perjuicio patrimonial se concreta a la "transferencia de cualquier activo patrimonial". Esto es, que el sistema informático o automatizado, alterado por las manipulaciones del agente, realiza la transferencia de una parte del patrimonio o, en el caso de los cajeros automáticos, la entrega del efectivo.

Por cierto, esta conducta que tipifica la "manipulación" informática con ánimo de lucro comprende la conducta prevista en el hurto telemático ya que este concepto es tan genérico que comprende el uso de la telemática. Hay que tener en cuenta que frente al surgimiento de las nuevas manifestaciones criminales que utilizaban la tecnología, los legisladores respondieron, desde el Código Penal peruano, como hurto agravado y, en las legislaciones europeas, como estafa o fraudes para adptarlas a las manipulaciones informáticas. El problema central es que ambas soluciones afrontan únicamente el problema de las afectaciones del patrimonio individual y no el complejo problema de la criminalidad tecnológica o informática.

[273] Cfr. Romeo Casabona, Carlos. Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías. En: Poder Judicial. Número 31. Setiembre 1993, p.185.
[274] Vives 415.

Por otro lado, el tipo penal de hurto telemático afronta el problema correctamente y ha demostrado eficiencia y utilidad para sancionar estas conductas desde 1991, pues la jurisprudencia ha entendido que el uso de la telemática puede comprender tanto la trasnferncia no consentida de fondos[275] como la información con valor económico[276]. Mientras que la estafa informática tambien es útil para afrontar la afectación del patrimonio personal al superar los límites del engaño y error de la estafa clásica. Incluso, desde una perspectiva político criminal pueden coexistir estas dos conductas ya que la estafa, por manipulaciones informáticas, puede proteger el patrimonio en su conjunto y el hurto telemático sancionar la transferencia no consentida de fondos.

4.1.6.3.2. La tecnología como medio defraudatorio. Estafas on line.

Las nuevas manifestaciones de la criminalidad que utiliza los sistemas informáticos han encontrado un nuevo y muy eficaz medio para defraudar en el sentido clásico de la estafa.

Donna[277] nos recuerda que nos encontramos ante un supuesto de estafa "cuando la máquina ha sido preparada para, aun recibiendo el importe requerido, no entregar el dinero, la cosa o prestar el servicio", pues en ese supuesto la máquina arreglada es el medio que utiliza el agente para engañar y hacer incurrir en error a otra persona quien utiliza la máquina. Es decir, la máquina sólo es un medio para engañar y hacer incurrir en error a otra persona.

Además de las conductas propiamente de manipulación de elementos informáticos, la Internet o los elementos tecnológicos pueden ser un nuevo medio para cometer estafas clásicas con mayor eficacia y a un número elevado de

[275] Cfr. Ejecutoria Superior en Rojas Vargas, Fidel. *Delitos contra el patrimonio*. Nota 161.
[276] Cfr. Ejecutoria Superior en Rojas Vargas, Fidel. *Delitos contra el patrimonio*. Nota 164.
[277] Dona Ob. Cit. p. 69.

personas. La delincuencia se ha adaptado a los nuevos tiempos y utiliza la tecnología[278] para perfeccionar sus timos y difundirlos a través de la red difunden diversos mensajes ofreciendo subastas de productos por internet, oportunidades de empleo, fraudes del paquete vacacional, fraudes telefónicos, fraudes de phising informático, el fraude de los escolares literatos, haber ganado una lotería de Microsoft, que se es beneficiario de una herencia o donación, la encomienda de DHL o la famosa "estafa nigeriana".

Se demuestra, pues, que la tecnología es un medio para perfeccionar el engaño creando una especial *mise en scene* el cual recae en una persona física quien incurre en error y realiza la disposición patrimonial. Efectivamente, aunque estas conductas se valgan de la internet y el computador para sus actividades ilícitas, se tiene a una persona física que abre el correo, lo responde, cae en el error al creer que está realizando un buen negocio o adquiriendo un producto y, finalmente, realiza la disposición patrimonial. De esta manera, estas conductas se subsumen perfectamente en la estafa clásica.

A continuación, presento, en base a la casuística extraída del interesante libro del Cmte PNP Henry Huerta[279], con las cuales se demuestra que la tecnología es un medio para perfeccionar el engaño creando una especial *mise en scene* el cual recae en una persona física quien incurre en error y realiza la disposición patrimonial. Estas conductas aunque se valgan de la internet y el computador se tiene a una persona física que abre el correo, lo responde, cae en el error al creer que esta realizando un buen negocio o adquiriendo un producto y, finalmente, realiza la disposición patrimonial. De esta manera, estas conductas se subsumen perfectamente en la estafa clásica.

[278] Cfr. Huerta Casaverde, Henry. *La estafa y otras defraudaciones…* p. 229 y ss.
[279] Ob cit. p. 239 y ss.

4.1.6.3.3. Las nuevas conductas defraudatorias con el uso de la tecnología.

a. Fraudes telefónicos[280].

En este rubro se debe considerar las llamadas telefónicas mediante las cuales se solicita dinero para liberar a un familiar detenido por ocasionar un accidente de tránsito u otro ilícito o haber sido intervenido en aduanas. Asimismo, la modalidad mediante la cual el estafador se hace pasar como el dueño de casa y solicita a la empleada que saque algunos bienes.

b. Subasta por internet.

Se difunden, vía la red, supuestas subastas en la cual se ofrecen productos. Al resultar favorecido de la subasta se informa al usuario que deposite la suma de dinero en una cuenta, pero recibe un producto de características inferiores al ofrecido o sin ningún valor.

c. Los timos de ISP (Proveedores de Servicios de Internet)

Los proveedores de servicios registran el nombre de dominio de un usuario como propio para obligarlos a continuar prestándole los servicios.

d. El cuento de gane dinero trabajando desde su propia casa.

Los estafadores ofrecen una oportunidad de ganar dinero trabajando desde su casa prometiendo altos ingresos pero les piden que, para comenzar el negocio, deben comprar productos. Luego de esta compra las víctimas se dan cuenta que es un fraude.

[280] Esta modalidad incluso ha traspasado las fronteras pues delincuentes peruanos, con información obtenida en las colonias peruanas, llaman por teléfono desde el exterior solicitando dinero para ayudar a un familiar supuestamente detenido en el extranjero. Cfr. www.larepublica.pe/30-03-2013/peruanos-estafan-desde-el-extranjero-con-solo-una -llamada

e. Fraude del paquete vacacional.

Se ofrecen paquetes de viaje con alojamiento y viajes de alta calidad, pero al llegar al destino se dan con la sorpresa que los servicios son de inferior calidad e incluso se han realizado cargos a la tarjeta de crédito por conceptos no contratados ni suministrados.

f. La estafa nigeriana.

Este fraude conocido también como el "timo 419" (en alusión al artículo del Código Penal Nigeriano que prevee la estafa), se inició en los años 70`s, consiste en enviar primero por carta, luego vía fax y ahora por correo electrónico un mensaje comunicando que necesitan su apoyo para sacar una fuerte cantidad de dinero de Nigeria a cambio de una generosa recompensa. Sin embargo, se solicita a la víctima que envíe una suma de dinero para algunos gastos como sobornos u otros gastos operativos; sin embargo, una vez obtenido el dinero el estafador corta toda comunicación.

Este es un ejemplo claro de la manera en que los delincuentes se adaptan a la tecnología utilizándola para sus ilícitos propósitos.

Esta estafa tiene algunas variantes respecto al motivo para solicitar dinero. Entre ellos, el militar en Irak que desea invertir altas sumas de dinero para adquirir inmuebles; el timo de la lotería en el cual anuncian a la víctima que ha ganado el premio mayor de la lotería; la compensación de la estafa nigeriana mediante la cual le anuncian que el gobierno nigeriano le indemnizará por haber sido la víctima de la "estafa nigeriana"; o la novia rusa quien envía una solicitud de amistad con provocativas y sensuales fotos mediante las cuales se atraen a incautos para pedirles dinero con diversos pretextos.

g. Fraude de los escolares literatos.

En este caso, los miembros de una editorial visitan diferentes colegios auspiciando un supuesto concurso escolar de literatura y solicitan a los niños que participen escribiendo un relato. Unos días más tarde, llaman a los padres para comunicarles que su hijo ha ganado el concurso y debe abonar entre 25 a 50 nuevos soles para editar el libro con los cuentos ganadores. Sin embargo, el concurso nunca existió y nunca se publica el libro con todos los participantes.

h. Fraude por manipulación de máquinas.

Es una variante de la antigua adulteración de artefactos que cuentan con medidores o contadores como los taximetros, básculas o medidores de luz o agua en los cuales se manipula o altera el sistema para defraudar al usuario. Asimismo, cuando el propietario de un negocio o de una máquina expendera de productos la "arregla" para recibir el dinero pero no entrega el producto produciendo un perjuicio patrimonial.

i. La interceptación de llamadas[281].

En esta novísima modalidad de apropiarse de lo ajeno obtienen información de cuentas bancarias y los datos de sus titulares. Con esta información y con documentos falsificados se presentan al banco y realizan una transferencia de dinero y cuando el funcionario bancario llama por teléfono al titular de la cuenta para confirmar la autenticidad de las transferencias pero esta llamada es interferida por otro delincuente quien se hace pasar por el verdadero titular y autoriza la transferencia.

[281] Cfr. Peru 21, edición del jueves 11 de abril de 2013.

4.1.6.3.4. Conductas que utilizan tarjetas de crédito o de débito que con bandas magnéticas.

Unas de las principales conductas que utilizan los criminales tecnológicos y además uno de los medios más antiguos para apropiarse del patrimonio ajeno se encuentran relacionados al uso de tarjetas electrónicas o con bandas magnéticas como las de crédito, de débito o las que sirven para obtener las que utilizan bandas magnéticas en el cual guardan la información. Los delincuentes utilizan un pequeños aparato denominado "Skinner" con el cual copian la información de la banda magnética de una tarjeta de crédito. Esta información se transfiere a una banda magnética la cual se adhiere a otra tarjeta plástica falsificada con la cual efectúan pago de servicios, transferencias de fondo, obtienen disposición de efectivo en los cajeros o adquieren productos.

El uso abusivo de tarjetas magnéticas tiene un tratamiento próximo a los fraudes informáticos.

Las entidades bancarias emiten diversas tarjetas de banda magnética que pueden ser de crédito en base a una línea de crédito que se le otorga previamente en base a una calificación de sus capacidades de pago, las tarjetas de débito con las que se puede pagar bienes o servicios u obtener dinero que el titular tiene depositado en su cuenta bancaria o las tarjetas prepagadas que con las cuales se puede pagar hasta el límite del valor de las tarjetas.

a. Obtención fraudulenta de tarjeta de crédito. En el cual el sujeto se presenta a la entidad bancaria para solicitar una tarjeta de crédito con su correspondiente línea de crédito. Aquí no se trata de un engaño de la estafa ya que esta conducta se encuentra tipificada en el artículo 247, obtención fraudulenta de financiamiento.

b. Tarjetas de crédito ajenas o clonadas. El uso de tarjetas clonadas, es decir, que se ha copiado la información de la banda magnética de una tarjeta de crédito o débito mediante el cual se obtiene la compra de bienes o servicios. En este caso se emplea una conducta engañosa aparentando tener crédito e induciendo a error a los empleados de las casas comerciales quienes creen que están realizando una transacción con el titular de la tarjeta.

Respecto a este punto, se debe tener en cuenta que las tarjetas que utilizan bandas magnéticas que contienen la información de un titular de una cuenta bancaria puede ser un medio idóneo para engañar a un empleado de un establecimiento comercial, pues el delincuente se presenta como titular y obtiene bienes o servicios.

En cambio, si el agente utiliza una tarjeta de débito o crédito ajena o clonada para obtener dinero de un cajero automático o terminal POS, esta conducta se encuadra en el hurto telemático ya que el uso indebido de estos dispositivos emplean la telemática para lograr el apoderamiento de dinero.

c. Uso de tarjetas de crédito por encima del límite de la línea de crédito. Bajo[282] nos informa que el Tribunal español ha considerado como delito de estafa cuando un sujeto "utiliza la tarjeta a sabiendas de que el crédito en ella otorgado se hallaba agotado, representa utilizar una apariencia engañosa fingiendo crédito que no tenía, consiguiendo inducir a error a diversos comerciantes…" aunque Bacigalupo considera que "no hay acción concluyente del tenedor de la tarjeta" contra el dependiente del establecimiento comercial ya que éste acepta la tarjeta confiando en la solvencia del banco.

d. Las tarjetas prepago con dinero. De la misma manera que las tarjetas telefónicas o electrónicas que permiten el pago de servicios como la del metropolitano no se

[282] Cfr. Bajo Fernández, Miguel. *Manual de Derecho penal…* p. 187.

encuadran ni en la estafa porque se activa sobre una máquina o sensor ni en el hurto telemático porque no hay transferencia electrónica de fondos ni la violación de claves secretas. En efecto, quien utiliza una tarjeta con lector manipulado para acceder al servicio actúa sobre una máquina sin intervención de persona alguna.

Estas conductas no se subsumen en el tipo de estafa porque no concurre el engaño[283] que ocasiona un error entendido como el estado psicológico en el que incurre una persona a consecuencia de aquel.

4.1.7. Daños.

> **Artículo 205.-** El que daña, destruye o inutiliza un bien, mueble o inmueble, total o parcialmente ajeno, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a sesenta días-multa.

Sujeto activo

Puede ser cualquier persona.

Bien jurídico

Se trata de la propiedad[284].

Apectos objetivos

Este delito gira en torno a tres verbos, dañar, destruir o inutilizar, que definen conductas que buscan afectar en diverso grado tanto el funcionamiento de una cosa con las cuales se disminuye su valor patrimonial. Aunque esta podría haberse definido perfectamente con dos verbos centrales; dañar y destruir.

[283] Cfr. Bajo Fernández, Miguel. *Manual de Derecho penal*… p. 185
[284] Cfr. Bramont Arias Torres / García Cantizano, María. *Manual de Derecho penal*… p. 383

Dañar está referido a disminuir el valor patrimonial de una cosa comprometiendo primordialmente la materia con la que ha sido hecha. Sin embargo, Bramont Arias Torres y García Cantizano[285] nos recuerdan la precisión de Soler, quien afirma que no toda alteración causada a un bien se equipara a esta conducta, sino solo será considerado delito de daños la que subsiste de manera indeleble o considerablemente fija, de modo que su reintegración del bien a su anterior estado represente algún esfuerzo o trabajo apreciable y, además solo es necesario disminuir irreparablemente su calidad o la posibilidad de usarla.

Inutilizar, en las precisas palabras de Roy Freyre[286], es afectar fundamentalmente la función para la que servía. En rigor, inutilizar es sinónimo de dañar pues en ambos supuestos la acción del agente está dirigida a evitar el normal funcionamiento o uso de una cosa. Cuando se daña o inutiliza una cosa se estropea o perjudica momentáneamente su valor.

Destruir es desaparecer el objeto o reducirlo a escombros y por lo tanto pierde todo su valor económico. Con esta acción ya no es posible reparar o reconstruir la cosa.

Objeto material.

La acción recae sobre cualquier bien, mueble o inmueble. Los bienes muebles son bienes tangibles o corpóreos sobre los cuales se deteriorar o malograr por medios físicos debido a lo cual se excluyen los elementos inmateriales como el software o los elementos lógicos que componen el sistema informático[287]. El profesor Roy Freyre agrega que el bien además de tener corporeidad debe ser total o parcialmente ajena[288].

---

[285] Cfr. Bramont Arias Torres / García Cantizano, María. *Manual de Derecho penal*… p.384.
[286] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 332
[287] Cfr. Gutierrez Frances, Mariluz. Notas sobre la delincuencia informática: Atentados contra la "información" como valor económico de empresa. En Derecho Penal Económico y de la Empresa. p. 411.
[288] Cfr. Roy Freyre, Luis, *Delitos contra el patrimonio*… p. 333.

El objeto material de esta conducta recae en una cosa mueble o inmueble en su sentido clásico; esto es, corpóreo[289] que ocupa un lugar en el espacio, susceptible de ser desplazado, aprehendido o percibido por los sentidos y el bien inmueble. El concepto ampliado de cosa mueble del hurto no puede ser utilizado para interpretar este tipo penal pues se encuentra restringido a los delitos de hurto. Este concepto puede comprender a las máquinas, pantallas, memorias que forman parte del hardware de un sistema informático empero, los datos, el software o la información contenida en el sistema informático no se encuentran incluidos en dicho artículo y, en virtud del principio que prescribe la analogía en el Derecho Penal no podemos extender el concepto de cosa mueble a los datos, o los programas que forman parte del software.

Un sector de la doctrina propone la reinterpretación del delito de daños[290] para afrontar los problemas del sabotaje informático a partir de considerar que ese tipo penal no exige la materialidad de la cosa mueble o inmueble que se traduzca en "aprehensividad" en el sentido de los delitos de apoderamiento. Lo verdaderamente relevante, nos informa Gutierrez Frances, es que "se deteriore o dañe algo valorado económicamente" con lo cual se puede incluir a los elementos lógicos de los sistemas informáticos como objeto material del delito de daños.

En conclusión, se debe tipificar el delito de daños informáticos para sancionar las conductas que afecten los elementos lógicos o la información contenida en soportes o los elementos lógicos que integran un sistema informático.

4.1.7.1. EXCURSO: Los daños o el sabotaje informático.

En la doctrina, especialmente la alemana y la española se utiliza la expresión de "sabotaje informático" para denominar la acción de dañar, destruir o alterar los

[289] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*... p. 333. Bramont Arias / García Cantizano, María. *Manual de Derecho penal*… p.383

[290] Cfr. Gutierrez Frances, María Luz. *Notas sobre la Delincuencia Informática*... p. 411 y ss.

elementos lógicos que integran un sistema informático. Por mi parte, considero que es mejor utilizar el vocablo "daños", porque "sabotaje" resulta excesiva ya que significa, de acuerdo a la RAE, "daño o deterioro en instalaciones o productos que se hace como procedimiento de lucha contra patronos en un contexto de conflicto social o político. En consecuencia, prefiero utilizar la denominación "daños informáticos" por ser un *nomen iuris* inequívoco.

La nueva conducta, surgida como una expresión típica de la era informática se conoce como la "destrucción o inutilización del soporte lógico, esto es de datos y programas contenidos en un ordenador o en sus bandas magnéticas[291] que se consigue con la introducción de programas crash, virus, time bombs, u otras rutinas capaces de afectar los elementos lógicos, el software o la información.

Los daños informáticos se refieren a destruir o inutilizar el software o la información y pueden ser permanentes o temporales ya sean que afecten intereses de una persona natural o de una persona jurídica. Es la inutilización (que hace imposible su uso) del soporte lógico del ordenador, pues estas afectan su operatividad sin dañar el soporte o el ordenador. [292]

Como se sostiene en la doctrina española, son sabotajes informáticos capaces de causar un perjuicio empresarial valuable económicamente,[293] es la destrucción o alteración de la sustancia de la cosa que tenga interés para la propia existencia de la misma.

Por las características propias del delito de daños informáticos, no es necesario que se afecte o ponga el patrimonio ni la acción disminuya su valor total o parcialmente aunque en algunos casos se verifique esta pérdida patrimonial, pues

[291] Cfr. Romeo Casabona, Carlos. *Delitos cometidos con la utilización de tarjetas de crédito*… p.201.
[292] Cfr. Romeo Casabona, Carlos. *Delitos cometidos con la utilización de tarjetas de crédito*… p.203.
[293] Cfr. Gutierrez Frances, María Luz. *Notas sobre la Delincuencia Informática…* p. 293.

lo verdaderamente importante es que se ponga en peligro la seguridad e intangibilidad de la información tratada informáticamente.

Por tal razón, concuerdo conque el objeto material -por así decirlo, ya que se tratan de elementos inmateriales- son el soporte lógico (elemento físico, incorporal) y la información tratada o almacenada del sistema informático: ésta es la cualidad de datos y programas, que son meros impulsos eléctricos plasmados normalmente en un soporte material (la banda o disco magnéticos).[294]

De otro lado, no es necesario que éstos tengan o no valor económico ya que en los daños informáticos no se protege el patrimonio aunque puede tipificarse como una conducta agravada cuando, además de dañar los elementos informáticos, se ocasiona un perjuicio patrimonial.

Se puede apreciar las siguientes modalidades:[295]

1- Borrar o cancelar: hacer los datos ilegibles de forma irrecuperables
2- Ocultar: impidiendo de forma duradera o temporal el acceso a los datos por los sujetos autorizados para ello, no utilizables
3- Inutilizar: es la trasnsformación de los datos de modo que su utilidad se menoscaba o interrumpe, es decir, que no se pueda alacanzar de modo adecuado o correcto su finalidad.
4- Alterar: cambiar el contenido de los datos o de las órdenes.

4.1.7.2. Diferencia entre el delito de daños contra el patrimonio individual y el daño informático se encuentra en el bien jurídico tutelado y en objeto material. En

[294] Cfr. Romeo Casabona, Carlos. *Delitos cometidos con la utilización de tarjetas de crédito*… p.202.
[295] Cfr. Corcoy Bidasolo, Mirentxu. *Legislación Penal sobre protección de la criminalidad*… p. 145.

el caso de los daños patrimoniales el bien jurídico es el patrimonio individual mientras que en los daños informáticos se protege la integridad o seguridad de los datos informáticamente tratados o almacenados. Por otro lado, en los daños patrimoniales la acción recae en la cosa mueble en el sentido clásico como objeto corpóreo y en los daños patrimoniales la acción recae sobre los elementos lógicos como el software o la información que contiene el sistema.

Por ello, concuerdo en que "la destrucción de datos tratados informáticamente" debe ser un delito autónomo[296] y no reinterpretar la conducta de daños contra el patrimonio.

Aspecto subjetivo.

El delito de daños solo puede realizarse con dolo directo[297]. Esto es conocimiento y voluntad que se está dañando una cosa total o parcialmente ajena. Sin embargo, no existe un ánimo de lucro ni el agente se enriquece u obtiene algún beneficio de su acción.

4.1.8. Delitos contra los derechos intelectuales.

4.1.8.1. Delitos contra los derechos de autor y conexos.

4.1.8.1.1. Edición Ilegal.

> **Artículo 216.-** Será reprimido con pena privativa de libertad de uno a dos años ni mayor de cuatro años y de diez a sesenta días-multa, a quien estando autorizado para publicar una obra, lo hiciere de las formas siguientes:
>
> a) Sin mencionar en los ejemplares el nombre del autor, traductor, adaptador, compilador o arreglador.
> b) Estampe el nombre con adiciones u supresiones que afecten la reputación del autor como tal o, en su caso, del traductor, adaptador, compilador o arreglador.
> c) Publique la obra con abreviaturas, adiciones, supresiones, o cualquier otra modificación, sin el consentimiento del titular del derecho.

[296] Cfr. Gutierrez Frances, María Luz. *Notas sobre la Delincuencia Informática…* p.414.
[297] Cfr. Roy Freyre, Luis. *Delitos contra el patrimonio*… p. 333.

d) Publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto; o las publique en conjunto, cuando solamente se le haya autorizado la publicación de ellas en forma separada.

El uso de la informática y la tecnología constituyen medios útiles y eficaces para afectar el bien jurídico, especialmente en las reproducciones de copias ilegales, ya que la tecnología facilita la duplicación de un número casi ilimitado de copias.

Bien jurídico.

En este capítulo se tutela el "derecho de autor" en sus manifestaciones patrimoniales y morales de las obras literarias o artísticas. Esto es, el derecho del autor o titular de los derechos a autorizar su publicación y que en éstas se reconozca su autoría. La Constitución Política del Perú garantiza, en su artículo 2 inciso 8, como derecho fundamental el derecho a la propiedad intelectual por lo que corresponde cautela el derecho exclusivo que tiene el autor para disponer de su obra. Por su parte la ley de derecho de autor, Decreto Legislativo Nº 822 artículo 8, excluye de la protección del derecho de autor a algunas obras.

El derecho a la propiedad intelectual otorga al autor la exclusividad de explotar o transferirla y tiene dos aspectos; derechos patrimoniales y derechos morales. Los patrimoniales estan referidos a obtener un lucro y los derechos morales o el derecho de paternidad de la obra le permite ser reconocido como el creador de la obra. De este derecho se derivan otros como, a la divulgación, al anonimato, al reconocimiento de la paternidad, al respeto de la obra, a la modificación y a la retractación.

En el plagio se reconoce el aspecto moral del derecho de autor de manera que se respete el derecho del autor a ser reconocido como tal.

Sujeto activo.

Se trata de un sujeto activo especial. Solo puede ser cualquier persona que cuente con la autorización para publicar una determinada obra.

Elementos objetivos.

Este tipo penal sanciona diversas conductas que afectan el derecho moral ya que, aunque existe una autorización para publicar una obra se realiza alterando su contenido o sin colocar el nombre del autor. Se trata de una publicación en condiciones distintas a las autorizadas por el autor de la obra que afecta su derecho moral.

La norma penal permite que se comprendan las obras en cualquier tipo de soporte tecnológico o informático.

Objeto material.

Es la obra y sus reproducciones que se encuentra definido en el Decreto Legislativo Nº 822, Ley de Derecho de autor, se la define como: "Toda creación intelectual personal y original, susceptible de ser divulgada o reproducida de cualquier forma, conocida o por conocer." Esta concepción tan amplia admite las reproducciones realizadas por cualquier forma que facilita la tecnología.

Elemento subjetivo.

La acción debe realizarse con dolo directo. El agente debe conocer que esta editando una obra en la cual no se ha consignado el nombre del autor o ésta tiene supresiones o modificaciones.

Consumación.

La conducta se perfecciona al momento que se publique las obras en las condiciones descritas en los incisos del artículo 216. La publicación se refiere a difundir o poner la obra a disposición del público.

4.1.8.1.2. Reproducción y distribución de copias ilegales.

> **Artículo 217.-** Será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que con respecto a una obra, una interpretación o ejecución artística, un fonograma, o una emisión o transmisión de radiodifusión, o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza alguno de los siguientes actos, sin la autorización previa y escrita del autor o titular de los derechos:
>
> a. La modifique total o parcialmente.
> b. La distribuya mediante venta, alquiler o préstamo público.
> c. La comunique o difundida públicamente, transmita o retransmita por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.
> d. La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.
>
> La pena será no menor de cuatro años ni mayor de ocho y sesenta a ciento veinte días multa, cuando el agente la reproduzca total o parcialmente, por cualquier medio o procedimiento y si la distribución se realiza mediante venta, alquiler o préstamo al público u otra forma de transferencia de la posesión del soporte que contiene la obra o producción que supere las dos (2) Unidades Impositivas Tributarias, en forma fraccionada, en un solo acto o en diferentes actos de inferior importe cada uno

Sujeto activo.

Cualquier persona pues no cuenta con la autorización del autor. Sin embago, en el inciso "d", se requiere de un sujeto activo especial ya que el agente deberán contar con la autorización para publicar las obras.

Elementos objetivos.

La edición ilegal se produce cuando se altere, difunda sin autorización del titular del derecho. En el inciso "d" se refiere a la reproducción de un número superior a los autorizados.

Se admite el uso de medios informáticos.

4.1.8.1.3. Plagio.

> **Artículo 219.-** Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a ciento ochenta días - multa, el que con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena.

Sujeto activo.

Cualquier persona. El tipo penal no requiere de ninguna calidad especial.

Bien jurídico.

Se afecta tanto los derechos patrimoniales como los derechos morales del autor de una obra.

Tipo objetivo.

El plagio o la copia de obras ajenas tiene dos modalidades:

1. Atribuirse la titularidad o paternidad de una obra.
2. Atrbuir a otro la autoría de una obra.

Esta conducta puede utilizar las nuevas tecnologías o la informática.

Tipo Subjetivo.

Dolo directo.

Consumación.

Se realiza cuando el agente hace suya la obra o de otro distinto al autor.

4.1.9. Fe pública.

> **Artículo 427.-** El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho, con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años y con treinta a noventa días-multa si se trata de un documento público, registro público, título auténtico o cualquier otro transmisible por endoso o al portador y con pena privativa de libertad no menor de dos ni mayor de cuatro años, y con ciento ochenta a trescientos sesenticinco días-multa, si se trata de un documento privado.
>
> El que hace uso de un documento falso o falsificado, como si fuese legítimo, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas.

4.1.9.1. Falsificación de documentos.

El concepto de falsedad, entendido como falta u ocultamiento de la verdad del contenido de los documentos tanto en lo relativo a la falsedad material (sobre la autenticidad del documento) como en la falsedad ideológica (respecto a la información que contiene), resulta ser el aspecto común a todos los tipos legales que el Título XIX del Código Penal contiene. Aunque el rubro de los delitos contra la fe pública no cautela la existencia de la verdad en abstracto, sino de la veracidad jurídica.[298]

Sin embargo, es conveniente precisar que la simulación de un documento auténtico u otra conducta que afecta la fe pública, únicamente adquieren trascendencia jurídica cuando guardan "relación con el tráfico jurídico"[299].

---

[298] Cfr. Bustos Ramírez, Juan. *Manual de Derecho Penal*… Parte Especial. p. 337. 2da ed. Ed. Ariel. Barcelona. 1991. Este autor agrega que "tal veracidad jurídica aparezca indisolublemente ligada al concepto de autenticidad del objeto, justamente para que pueda dar fe pública."

[299] Cfr. Orts Berenguer, Enrique y otros. *Derecho Penal*, Parte Especial. 2da Ed. p. 654. Ed. Tirant lo Blanch. Valencia. 1996. Esta es la posición dominante en la doctrina cfr. Muñoz Conde, Francisco; *Manual de Derecho Penal* p. 556 Ed. Tirant lo Blanch. Valencia. 1995; Bustos, ob. cit. p. 337; Bramont Arias, Luis y García Cantizano, Ma. del Carmen. *Manual de Derecho Penal*… p.621.

Bien jurídico.

En los delitos contra la fe pública el bien jurídico tutelado es la fe pública, entendido como la funcionalidad del documento en el tráfico jurídico, en la medida que desarrolla una triple labor: perpetuación de la declaración documental, garantía del autor del documento en el tráfico jurídico y medio de prueba de la declaración documental.[300]

Esta posición se encuentra firmemente arraigada en la doctrina conforme señala Orts que sólo es posible concretar el bien jurídico protegido "cifrándolo en el tráfico jurídico"[301]. Asimismo, Bustos afirma que "El bien Jurídico fe pública tiene un carácter funcional"[302] más allá de una simple y pura tutela de la falta de verdad en los documentos.

OBJETO MATERIAL

El tipo penal señala que el objeto material sobre el cual recae la conducta descrita en el tipo objetivo es un documento.

4.1.9.2. El documento informático.[303]

Muñoz Conde[304] señala que "En un sentido amplio, documento es toda materialización de un pensamiento. En este sentido, documento es todo objeto que

[300] Cfr. Bramont Arias, ob. cit. p.624. En el mismo sentido Muñoz Conde, Francisco. *Código Penal – Parte Especial…* p.718, expone que "La importancia del documento en el tráfico jurídico es tal que puede considerarse que, más que la fe pública o la propia seguridad en el tráfico jurídico fiduciario, es la funcionalidad del documento mismo (en sus distintas formas de aparición en las relaciones jurídicas) el verdadero bien jurídico protegido en estos delitos." El concepto dominante de bien jurídico es criticado por Puppe quien considera que pretende comprender a todas las conductas que integran el título de los delitos contra la fe pública. y que en realidad cada conducta protege en concreto un interés distinto. Puppe, Ingeborg. La protección de documentos en la era informática. En Revista Peruana de Doctrina y Jurisprudencia Penales. Nº 03. 2002. p. 270.

[301] Cfr. Orts Berenguer, Enrique y otros. *Derecho Penal…* p. 659.

[302] Cfr. Bustos, ob.cit. p.337. En el mismo sentido Muñoz Conde, ob. cit. p. 557 agrega que: "la seguridad en el tráfico fiduciario, que es como suele denominarse, también el bien jurídico común a estos delitos".

[303] CPE. 26. A los efectos de este código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficiencia probatorio cualquier otro tipo de relevancia jurídica. Evolución del concepto de documento reconociendo el **"documento electrónico"**. Cfr. Gutierrez Frances, María Luz. Notas sobre la Delincuencia Informática…

sea capaz de recoger una declaración de voluntad o pensamiento atribuible a una persona y destinado a entrar al tráfico jurídico". En la misma línea de pensamiento García Cantizano acepta el concepto flexible, práctico, funcional del documento que se adapte a los nuevas exigencias de la tecnología que debe cumplir la misma función del documento tradicional "función garantista, probatoria o de perpetuación del documento"[305].

En la doctrina peruana se sostiene que documento es todo aquel medio que contiene con carácter de permanente una representación actual, pasada o futura del pensamiento o conocimiento o de una aptitud artística o de un acto o de un estado afectivo o de un suceso o estado de la naturaleza, de la sociedad o de los valores económicos, financieros, etc., cuya significación es identificable, entendible de inmediato y de manera inequívoca por el sujeto cognoscente.[306]

En nuestro ordenamiento jurídico, al no existir en el Código Penal un concepto propio de documento, podemos extraer su definición de las normas contenidas en el Código Procesal Civil. El código Procesal Civil tiene una concepción bastante moderna de documento[307] que incluye al electrónico o informático el cual, a pesar de tener un soporte inmaterial, perfectamente puede conservar y perpetuar información o declaración con el registro de su autor y se utiliza para probar o acreditar un hecho.

De este modo, en el artículo 233 del Código Procesal Civil señala que el documento es "todo escrito u objeto que sirva para acreditar un hecho". A continuación en el

---

[304] Muñoz Conde, Ob.cit. p. 580.
[305] MC García Cantizano p. 25.
[306] Cfr. Sánchez Velarde, Pablo. *Manual de Derecho Procesal Penal.* Idemsa, Lima 2006, pp. 698-699. De la misma opinión es Mixán Mass, Florencio; *La prueba en el procedimiento penal.* Ed. Jurídicas, Lima 1991, p.179.
[307] Cfr. García Cantizano, María. *La delincuencia informática…* p. 71.

artículo 234, señala las clases de documentos incluyendo cualquier clase de objeto donde pueda fijarse un hecho, acontecimiento o pensamiento. El aspecto esencial para considerar a un objeto en la categoría de documento es que tenga la capacidad para conservar o fijar en el tiempo un hecho o actividad humana

Por documentos se entiende todo objeto en el cual se ha fijado, por medio de signos que pueden ser interpretados o reconocidos por otros que tienen con permanencia jurídicamente apreciable, un contenido. No obstante, la protección penal recae únicamente sobre los documentos que poseen interés jurídicamente relevante cuando pueden servir como medios probatorios para fundamentar un derecho al ingresar al tráfico jurídico.

De otro lado, consideramos que son varias las razones que motivan el porqué simples fotocopias no pueden ser considerados documentos públicos; por un lado estrictamente procesal, es decir, por su ineficacia en el resultado: ¿qué sentido tiene investigar en base a una copia si no va a ser posible dictar una condena? y, por otro lado, porque una copia no es adecuada físicamente –como documento- para retener los datos que se pretende perpetuar.[308]

Así, se sostiene que es necesario que el documento sea adecuado objetivamente para tener efectos probatorios o algún tipo de relevancia jurídica. El objeto en que se fija el dato, hecho o narración ha de ser, sin embargo, por la característica de perpetuidad inherente al documento, idóneo para conservarlo durante cierto tiempo; no son, por tanto, soportes materiales idóneos para convertirse en documento, aquellos objetos con escasa capacidad de perpetuación de los datos

[308] De su parte, Rosales Artica, David. *El delito de falsificación de documentos*. En: Revista Actualidad Jurídica No.160, Gaceta Jurídica, Lima marzo 2007, p.132, sostiene que el objeto del delito es el documento (…) que incluye no solo a los papeles, sino también a los disquetes, discos, cintas de video y todo aquello que pueda recoger datos, declaraciones de voluntad o información, y que cumpla con las funciones de perpetuación, probatoria y de garantía.

que a ellos se incorporen.[309] Esto nos hace deducir que la simple copia o fotocopia de un documento original tampoco son adecuadas para producir efectos jurídicos.[310]

Hay que tener en cuenta también, que el artículo 185 del Código Procesal Penal, señala que son documentos los manuscritos, impresos, fotocopias, fax, disquetes, películas, fotografías, radiografías, representaciones gráficas, dibujos, grabaciones magnetofónicas y medios que contienen registro de sucesos, imágenes, voces; y, otros similares. Empero, consideramos que ello no se contradice con lo expuesto anteriormente ni con lo resuelto en las sentencias transcritas preliminarmente, puesto que existirá responsabilidad penal única y exclusivamente cuando existan medios probatorios (testimoniales, reconocimientos, confrontaciones, peritajes, etc.) plurales y convergentes que acrediten en forma indubitable y fehaciente la responsabilidad penal del procesado[311]. Es decir, la condena debe ser el resultado de una suficiente actividad probatoria que acredite sin lugar a dudas la responsabilidad penal del inculpado; bajo esta perspectiva, una simple fotocopia no puede ser sustento fehaciente para dictar una sentencia condenatoria.

En conclusión el documento electrónico reúne los requisitos establecidos por la doctrina:[312] i) es un método de perpetuar y constatar el contenido, ii) medio de garantía para conocer al autor y iii) sirve como prueba de su contenido.

Asimismo, existe una amplia normatividad que regula los documentos electrónicos y la administración de las bases de datos. La legislación peruana regula la emisión, conservación, autenticación de archivos que contengan microformas o información resguardada en cualquier soporte e incluso regula el uso de la firma digital o

[309] Cfr. Muñoz Conde, Francisco; *Derecho Penal…* pp.718-721.
[310] Cfr. Chocano Rodríguez, Reiner. *La falsedad documental del artículo 427 del CP.* En: Revista Peruana de Doctrina y Jurisprudencia Penal, IPCC, Grijley, Lima, 2000, p.496.
[311] Cfr. Cáceres J., Roberto; *Código Procesal Penal Comentado,* Jurista Editores, Lima 2006, p.254.
[312] Cfr. García Cantizano, Ma del Carmen. *Falsedades documentales…* p. 121.

electrónica. Desde el Decreto Legislativo Nº 681 (14.10.91) se reconoce que los elementos o formas procesadas por sistemas tecnológicos o informáticos tienen la calidad de documento con igual valor de los elaborados en papel. En la misma norma se determina que la falsificación y adulteración de microformas o sus duplicados serán reprimidas como delito contra la fe pública.

Posteriormente, se incorpora la firma digital como elemento que autentica los documentos electrónicos con la misma validez y eficacia que la firma manuscrita. Incluso el Decreto Supremo Nº 052-2008 PCM (19/07/08) establece la presunción de veracidad cuando aparece la clave privada del suscriptor.

5. SOBRE LA DENOMINADA LEY DE DELITOS INFORMÁTICOS. LEY N° 27309 (17.07.00).

> **Artículo 207-A.-** El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.
>
> Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

5.1. Bien jurídico

Para Luis Reyna el bien jurídico de este tipo penal sería la información contenida en los sistemas de tratamiento informatizado de datos que se le otorga a la información un valor económico.[313]

Bramont Arias Torres[314] considera que el bien jurídico es "la intimidad y concretamente la seguridad del tráfico de información".

Para Mazuelos[315] el bien jurídico es "la seguridad e intangibilidad del tráfico de información en la red".

Por mi parte, considero que "la seguridad informática" no es un bien suficientemente importante de protección y únicamente constituye el medio, no el objeto de protección.

---

[313] Cfr. Reyna Alfaro, Luis Miguel. *Los delitos informáticos*... p. 330
[314] Cfr. Bramont Arias Torres, Luis Alberto. *El delito informático*... p. 72.
[315] Cfr. Mazuelos, Julio. *Los delitos informáticos*... p. 301.

En rigor se protege, en el tipo base, la intangibilidad de la data o información contenida o tratada en un sistema informático tenga o no valor económico. En este contexto, la seguridad informática es el mecanismo de protección del bien jurídico. Esta afirmación se sustenta en que el tipo penal protege a cualquier tipo de información que se encuentra almacenado en un sistema informatizado, el cual resulta un interés que merece protección en una sociedad post industrial.

Desde 1991 el patrimonio individual se encuentra tutelado de posibles lesiones si las apropiaciones se efectúan por medios informáticos y pretende ser protegido por otras afectaciones por el segundo párrafo del artículo 207-A, cuando se exige que el intruso acceda a un sistema informático con el propósito de obtener un beneficio económico.

5.2 Elementos típicos del artículo 247 –A. Primer párrafo.

Tipo base.

5.2.1 Tipo objetivo

Sujeto activo.

Se trata de un sujeto activo común[316]. Aunque resulta evidente que el agente o el intruso debe tener conocimientos especializados de informática y conocer el manejo de computadoras, el tipo penal no exige que tenga alguna categoría especial, cualidad particular o cuente con estudios o títulos de alguna especialidad.

Acceso o ingreso no autorizado. La conducta central de este tipo penal se refiere concretamente a un acceso o ingreso no autorizado de una parte de un sistema computarizado.

[316] En el mismo sentido Mazuelos, Julio. *Delitos informáticos…* p. 297. Bramont Arias Torres, Luis. *El delito informático…* p. 73.

Este tipo penal no tipifica la conducta del hacker o intruso *per se*[317]. Es decir, aquel que simplemente ingresa o accede a un sistema informático sin autorización pero que no busca realizar ninguna acción posterior pues el legislador incluyó que el acceso o el uso indebido descrito en el artículo 207-A tenga una finalidad; realizar una acción lesiva concreta sobre la información que contiene un sistema informatizado; esto es alterar, modificar, copiar o acceder a información, etc. En consecuencia, para poder imputar este tipo penal se debe verificar que el acceso o uso indebido se haya tenido esta finalidad.

El carácter "indebido" del acceso se refiere al ingreso sin autorización o sin derecho[318]. Valladares, por su parte, agrega correctamente que: "el carácter indebido adjetiviza las conductas de ingresar o utilizar."[319] Este elemento, efectivamente, se relaciona directamente con el conocimiento de su ilicitud (dolo).

Al respecto, los sistemas informáticos usualmente tienen claves que permiten el acceso a los usuarios autorizados. En algunos casos puede permitirse el acceso a una página web, pero solamente a una parte de la información y la base de datos o información reservada se encuentra restringida a otros usuarios.

Ingresar es simplemente entrar o acceder al sistema o a una parte de un sistema informático. Es decir, cuando el sujeto se encuentre en capacidad de obtener la data que se guarda en él.

Por cierto, por las particulares características de la informática el acceso, interferencia o uso puede ser de manera remota o a través del internet.

---

[317] Mazuelos considera que la conducta de intrusismo informático se configura penalmente como un delito informático en el artículo 207-A. Cfr. Mazuelos, Julio. *Delitos informáticos…* p. 298.
[318] Cfr. Bramont Arias, Luis. *El delito informático*…, p. 72
[319] Valladares p. 310.

Se puede dar también el caso del usuario que tiene una autorización para ingresar a una parte del sistema pero, logra acceder a un nivel superior de seguridad o que contenga información sensible o reservada del sistema a cierta información pero no lo tiene para obtener o conocer.

Utilizar. Se refiere a la acción de emplear o servirse del sistema o de sus componentes. Bramont Arias Torres apunta que este supuesto se puede dar cuando el sujeto activo se encuentra dentro del sistema[320] y comienza o continúa usándola sin autorización.

Alterar, es modificar o cambiar la información o los programas de computación que contiene el sistema.

Interferir se refiere a la acción de introducirse en el sistema para perturbar, obstaculizar o evitar que la información sea transmitida.

Copiar no se requiere destruir la data o la información solo obtener una reproducción de ésta incluso sin dañarla o alterarla.

Objeto material. La conducta recae sobre los elementos informáticos ya sea los que integren el software o el hardware. Esto es, una terminal o cualquier elemento que componga un sistema de computadoras[321] Cualquier tipo de información. Ya sea que se encuentre almacenada en el disco duro, en un de almacenamiento externo, en la nube, se esté trabajando en la pantalla o se encuentre en transmisión.

[320] Cfr. Bramont Arias Torres, Luis. *El delito informático*... p. 72
[321] Cfr. Bramont Arias Torres, Luis. *El delito informático*... p. 73.

5.2.2 Tipo subjetivo

Dolo directo. El agente conoce que accede o utiliza una base de datos sin autorización. Adicionalmente el tipo penal incorpora un elemento subjetivo del tipo[322] cuando establece una finalidad específica o concreta como el fin de obtener, interferir, u obtener un beneficio económico.

Elemento subjetivo de intención precedente.

La deficiencia de este tipo penal constituye la exigencia de actuar "*con el fin de diseñar, interferir, copiar etc…*" ya que esto obliga al fiscal acreditar que el acceso se realizó con ese propósito específico quedando impune la conducta del intruso que simplemente ingresó por puro afán lúdico o por que no se pudo demostrar que el agente tenía la intención requerida en el tipo penal.

Sin embargo, esta forma de tipificar origina una serie de problemas. En primer lugar, no se sanciona el hacker o intruso[323]; en segundo lugar, resulta muy difícil acreditar el objetivo de acceder con el fin…. Por ello, hubiera sido preferible tipificar la conducta del acceso indebido o no autorizado como tipo base y como conductas agravadas la modificación, alteración[324] etc.

El mismo problema ocurre con el tipo agravado del artículo 207-A en el cual se describe la conducta de acceder "*con el fin de obtener un beneficio económico*".

---

[322] Cfr. Bramont Arias Torres, Luis. *El delito informático*... p. 73. En el mismo sentido, Valladares p. 312.
[323] Cfr. Reyna Alfaro, Luis Miguel. *Los delitos informáticos*… p. 332.
[324] Cfr. Reyna Alfaro, Luis Miguel. *Los delitos informáticos*… p. 335. Gutierrez Frances, advierte que la conducta del hacker se debe tipificar como "el mero acceso sin autorización a un sistema informático, desprovisto de toda intención de dañar o perjudicar de algún modo a otro." En: *Notas*… p. 421.

En mi opinión, considero que el acceso indebido debería ser una conducta punible *per se* sin esperar que esta actividad ocasiones algún perjuicio. Este adelantamiento de punibilidad es necesario por las características especiales del uso de la informática. Se debe considerar que el acceso pone en peligro real la información contenida en una base de datos o sistema informático.

5.2.3. Tipo agravado. Artículo 247 –A. Segundo párrafo

Se refiere al acceso indebido con el fin de obtener un beneficio patrimonial como un elemento subjetivo del tipo[325]. Se califica la acción de ingresar o usar cuando tiene como fin obtener una finalidad económica.

El tipo agravado se erige sobre los elementos del tipo base del artículo 207-A. Esto es, el agente ingresa indebidamente al sistema para alterar, ejecutar un programa con el propósito de obtener un beneficio económico. Con esta farragosa descripción la conducta típica contiene diversos requisitos que deben cumplirse.

En principio, el agente debe ingresar indebidamente o sin autorización del titular, a un sistema informático y realizar manipulaciones que permitan o faciliten la obtención de un beneficio económico. Esta agravante se refiere a una "manipulación informática irregular que genera una transferencia patrimonial" que se ha denominado en la doctrina, particularmente en la española como "fraude informático"[326]. Esto es, aquí se refiere no solo a la transferencia electrónica de fondos o el uso de la telemática sino a cualquier forma de obtener un beneficio económico de manera más amplia, que el hurto telemático. Asimismo, existe también una diferencia respecto al objeto materia de este delito, pues mientras en el hurto telemático se refiere exclusivamente a los "fondos", esto es, dinero

[325] Cfr. Bramont Arias Torres, Luis. *El delito informático*… p. 73.
[326] Cfr. Mazuelos, Julio. *Delitos informáticos*... p. 311 y ss.

contable; en esta conducta el beneficio económico puede ser cualquier elemento con valor patrimonial que integre el patrimonio personal.

Sin embargo, la agravante no está definida como un delito de resultado sino que nuevamente se exige un elemento subjetivo de intención trascendente.

5.2.5. Consumación.

Se trata de un delito de mera actividad[327]. Cuando se realiza las conductas descritas en el tipo penal[328]. No es necesario alterar, interferir u obtener el beneficio económico.

5.3. Elementos típicos del artículo 247 –B.

> **Artículo 207-B.-** El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

5.3.1 Bien jurídico.

Bramont Arias Torres considera que: "se protege el patrimonio puesto que la finalidad en el tipo penal es la de dañar el objeto material, esto es base de datos, sistema, red o programa de computadoras o cualquier parte de la misma.[329]"

Por mi parte, considero que el objeto de esta norma es proteger un bien jurídico supraindividual y no el patrimonio personal. Esto es, la información informáticamente tratada o almacenada. Este es el centro de protección ya que la conducta está dirigida a alterar, modificar o destruir la clase de información y

[327] Cfr. Mazuelos, Julio. *Delitos informáticos*… p. 305.
[328] Cfr. Bramont Arias Torres, Luis. *El delito informático*... p. 73.
[329] Cfr. Bramont Arias Torres, Luis. *El delito informático*… p. 72.

aunque en algunos casos pueda perjudicarse información con valor económico, no se puede afirmar que se intente proteger al patrimonio[330].

5.3.2. Tipo objetivo

Sujeto activo.

De igual manera que el artículo 207-A no se requiere calificación especial del sujeto activo por lo que puede ser cualquier persona la que realice la acción descrita[331].

5.3.3. Daños al sistema informático.

La conducta de sabotaje[332] o daños informáticos se realiza sobre la base de las conductas de intrusismo informático ya definido en el artículo 207-A pues que la conducta central es, nuevamente, el acceso indebido o no autorizado pero esta vez con el objeto o la finalidad de alterar, dañar o destruir. Sin embargo, existe también una coincidencia en la conducta del artículo 207-A en el cual se refiere "alterar un esquema u otro similar" el cual, por cierto, es una expresión que corresponde al daño informático ya que "alterar" es una forma de estropear, descomponer o modificar algo.

---

[330] Valladares considera que al dañar o alterar el sistema se afecta el valor económico de un sistema de computadores sin tener en cuenta que lo que realmente se afecta es la información, que es la que se altera o destruye. p. 313. Mazuelos, por su parte, sostiene que el bien jurídico tutelado es la seguridad e intagibilidad del tráfico de información en la red. *Delitos informáticos…* p. 309.

[331] Cfr. Mazuelos, Julio. *Delitos informáticos…* p. 306.

[332] El término "sabotaje" me parece excesivo para describir el daño a elementos informáticos debido a que esta expresión significa una acción desarrollada como forma de lucha en conflictos sociales o políticos. El viejo nomen iuris "daños" es perfectamente aplicable a las conductas que afectan, perjudicando, destruyendo o malogrando los elementos lógicos del sistema o la información almacenada o tratada en el sistema informático.

Mazuelos[333] considera que estamos ante un tipo especial del artículo 205 del código penal. Sin embargo, en el Código Penal se tipifica el delito de daños teniendo como objeto material los bienes muebles o inmuebles y, como ya vimos, los elementos lógicos como el software o la data de un sistema informático no encuadran en la categoría de bienes muebles y, además, en el artículo 205 se protege el patrimonio individual mientras que aquí se tutela un bien jurídico supraindividual.

Por otro lado, hay que subrayar que nuevamente el legislador tipificó este delito de acuerdo a la finalidad perseguida por el agente; en este caso, el acceso deberá tener como objetivo alterar, dañar o destruir una base de datos o programas informáticos. De esta manera, no se sanciona el daño o la destrucción del sistema informático, sino no se ingresó indebidamente al mismo.

"*Con del fin de alterarlos, dañarlos o destruirlos*". La conducta buscada por el intruso en este caso es estropear, descomponer o perturbar el normal funcionamiento del sistema. Por otro lado, el objeto material o sobre el cual recae la acción son el software, los elementos lógicos que componen un sistema o su data. No se refiere al hardware o sus elementos materiales ya que estos se encuentran protegidos por el delito de daños del artículo 205 del código penal.

Ciertamente, considero que la conducta de daños informáticos o daños al sistema informático debió ser tipificada como un delito de resultado, es decir, sobre la base concreta de ocasionar daños a un sistema o a los elementos que la integren, en la que se sancionen cualquier conducta que los altere, destruya o modifique.

[333] Cfr. Bramont Arias Torres, Luis. *Delitos informáticos*.. p. 308

Mazuelos[334] destaca que se presenta otro problema cuando el agente que ocasiona los daños informáticos fue autorizado a ingresar al sistema o se encuentra lícitamente en éste. En efecto, si éste ocasiona perjuicios o alteraciones al sistema, pero no ingresó ilegalmente al mismo, no podría imputarse esta conducta. Las imperfecciones anotadas evidencian las imperfecciones de esta norma penal que reclama ser inmediatamente modificada.

5.3.4. Tipo subjetivo

Al igual que la conducta descrita en el artículo 207-A se actúa con dolo directo y con el mismo elemento subjetivo de intención trascendente y, por lo tanto, adolece de la misma deficiencia anotada en el comentario del tipo base.

5.4. Elementos típicos del artículo 247 –C. Agravantes genéricas.

> **Artículo 207-C.-** En los casos de los artículos 207º-A y 207º- B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:
>
> 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo
> 2. El agente pone en peligro la seguridad nacional.

5.4.1 Bien jurídico.

El bien jurídico tutelado es el mismo que corresponden a las conductas previstas en los artículos 207- A y 207-B ya que en este artículo se repiten las conductas básicas y se agrega el plus de acceso aprovechándose del cargo o que ponga en peligro la seguridad nacional[335].

---

[334] Cfr. Mazuelos, Julio. *Delitos informáticos…* p. 307.

[335] De su lado, Reyna Alfaro, Luis Miguel. *Los delitos informáticos…* p.338, considera que en el tipo agravado se afecta a la información como valor económico. Sin embargo, el artículo 207-C por ningún lado

Por otro lado, en el inciso 2 se tutela también la seguridad nacional referida a que la información contenga aspectos valiosos o importantes para el desarrollo del país en un ambiente de estabilidad o tranquilidad, como data referida las instalaciones militares, sistema de armas o de defensa.[336]

5.4.2 Conductas agravadas.

Las circunstancias agravantes se refieren a dos condiciones:

- **Por la condición del sujeto activo**, se aprovecha del cargo utilizando la información privilegiada. Esta condición se refiere tanto a un funcionario público o un privado, pues lo relevante es que utilice su calidad o condición para lograr el acceso indebido. En palabras de Bramont Arias Torres[337] "la agravante gira en torno a un deber de lealtad" aunque resulte criticable el uso del término "información privilegiada" el cual ya se encuentra tipificado en el artículo 251-A del Código Penal.

- **Afecta la seguridad nacional**. En este supuesto la información que se altere, modifica o copie debe contener información sensible que afecte a la seguridad nacional. Al respecto, hay que tener presente que el tipo exige que la conducta no simplemente acceda o altere información referida a la seguridad nacional, sino que el agente ponga en peligro a la seguridad nacional.

---

menciona o hace siquiera referencia a esta cualidad. Por otra parte, se debe tener en cuenta que existe diferencia entre información con valor económico -que puede ser la que guarda información vital para la empresa- y la que representa un valor económico, como en el caso del dinero electrónico.

[336] Mazuelos advierte que el concepto de seguridad nacional ha servido para justificar la tipificación de conductas difusas y carentes de dañosidad vinculadas a un derecho penal del enemigo. Cfr. Mazuelos, Julio. *Delitos informáticos…* p. 315

[337] Cfr. Bramont Arias Torres, Luis. *El delito informático*… p. 74.

5.4.3. Consumación.

Respecto a la conducta de peligro a la seguridad nacional la conducta se consuma cuando se constate el peligro a la seguridad nacional. Es un delito de resultado, por lo que se admítela tentativa.

6. Los intentos de reforma de la Ley Nº 27309, Ley de delitos informáticos.

La denominada Ley de delitos informáticos Nº 27309 no consiguió solucionar ni abordar todos los problemas que introduce la tecnología y el uso de los sistemas informatizados, que es objeto de reforma en el Congreso de la República del Perú. Al respecto, se presentaron dos Proyectos de Ley el Nº 34/2011-CR, presentado el 11 de agosto de 2011, por el Grupo Parlamentario "Alianza por el Gran Cambio" a iniciativa del congresista Juan Carlos Eguren Neuenschwander; en adelante Proyecto Eguren y el Proyecto de Ley Nº 307/2011 presentado por el Grupo Parlamentario Fujimorista; el 05 de octubre de 2011, en adelante Proyecto Salazar.

6.1 Sobre el Proyecto Eguren[338].

Este proyecto pretende abordar los problemas penales ocasionados por el uso de la tecnología y los sistemas informáticos mediante una ley especial de la misma manera que se dictó la Ley Penal Tributaria y la Ley de Delitos Aduaneros. De acuerdo a este proyecto, una ley especial permite incluir aspectos procesales en la lucha de la criminalidad informática.

El Proyecto Eguren contiene una propuesta para regular las conductas que utilicen sistemas informáticos que, "por sus particularidades, requieren de una tipificación especial." De esta manera no se tipifican conductas en las cuales se utiliza la informática como medio sino solo se considera a "los delitos informáticos que

[338] Este proyecto transcribe información publicada en el sito web monografías.com sin verificar la calidad de la información y manteniendo los gruesos errores de la fuente.

afectan a los sistemas informáticos (la informática como objeto) y los supuestos en que se use sistemas informáticos para lesionar otros bienes jurídicos que no puedan reprimirse satisfactoriamente con los otros tipos penales contenidos en el Código Penal."

En principio, se propone derogar los artículos 186º segundo párrafo, inciso 3, sobre transferencias no autorizadas de fondos y los artículos 207º-A, 207º-B y 207º-C introducidos por la Ley de Delitos Informáticos. Además, incluye un Glosario de Términos con la finalidad de aclarar los vocablos que encierran conceptos técnicos empleados en esta propuesta.

Esta inicitiva ha sido recogida en el Predictamen de la Comisión de Justicia y Derechos Humanos.

Sin embargo, su principal debilidad es no plantear reformas a los artículos del Código Penal que contienen conductas que pueden ser realizadas utilizando medios informáticos. Las propuestas legislativas sobre la criminalidad tecnológica únicamente centran su interés en las nuevas conductas cometidas por medios tecnológicos, pero dejan de lado las ya tipificadas que deben ser reformadas para que puedan encuadrar, respetando el principio de legalidad, las nuevas manifestaciones criminales.

6.2 Sobre el Proyecto Salazar.

Este proyecto, de más modesto alcance, tiene por objeto tipificar nuevas figuras delictivas que utilicen tecnología de información y el secreto de las comunicaciones y Secreto Bancario y otorgar facultades a la Policía Nacional y el Ministerio Público en la investigación de estos delitos.

De esta manera de tipifica las siguientes conductas:

1. **Comercialización o difusión de bases de datos.**

Resulta necesario tipificar esta conducta, pues las bases de datos son las herramientas que necesita el delincuente tecnológico para cometer otros ilícitos. Se sanciona la comercialización, difusión o interceptación de las bases de datos que se encuentren en sistemas informáticos.

Sin embargo, en este tipo penal se incluye las conductas de modificaciones o introducción o difusión de virus en bases de datos, cuando los daños informáticos deben ser tratados en un tipo particular.

El objeto material es la base de datos o archivos que se encuentran tratados o alojados en sistemas informáticos.

2. **Prestación de servicios para sabotaje informático.**

Se sanciona la posesión, distribución, el desarrollo o distribución de programas, enlaces o páginas electrónicas que permiten obtener valores o beneficios económicos. De esta manera se pretendería sancionar el phising aunque de manera confusa, ya que resulta muy poca claro la posesión o distribución con el objeto o propósito de obtener beneficios u otros fines ilícitos.

Por otro lado, el *nomen iuris* no guarda relación con la conducta descrita, ya que el sabotaje o daños informáticos no busca necesariamente obtener un beneficio económico o un fin ilícito ulterior.

La inclusión de elementos subjetivos de intención trascendente dificultan la identificación de los elementos subjetivos que se encuentran en la actual ley de delitos informáticos y que han sido criticados en el apartado de esta tesis.

3. **Posesión de equipos de sabotaje informático.**

El objeto material del delito son las tarjetas magnéticas, electrónicas, otras análogas o sus componentes

Igualmente el nomen iuris de esta conducta no guarda relación con las conductas descritas en este tipo penal, ya que el sabotaje informático está vinculado con los daños a los sistemas informáticos, los programas o componentes y en este artículo se sanciona la elaboración o distribución de tarjetas magnéticas, sus elementos, data o instrumentos para fabricarlas.

4. **Delitos agravados por el uso de las TICs**

Se introduce una agravante genérica respecto al uso de software, hardware u otros elementos de las tecnologías de la información y la comunicación en la comisión de algún delito.

5. **Modificaciones al artículo 207 – C.**

Se propone modificar algunas circunstancias agravantes a la Ley de Delitos Informáticos.

6. **Aspectos procesales**

Incluye aspectos procesales para la persecución de estos delitos, entre ellos el "agente encubierto" sin tener en cuenta que esta figura se encuentra prevista (y vigente en el 80% del territorio nacional) en el artículo del Código Procesal Penal de 2004. Del mismo modo, la previsión del artículo 8 del Proyecto Salazar no toma en cuenta que la dirección de la investigación preliminar del Fiscal se encuentra definido en este cuerpo legal.

6.3 Sobre el predictamen de la Comisión de Justicia y Derechos Humanos del Congreso de la República del Perú.

Los Proyectos Eguren y Salazar obtuvieron un predictamen que ha sido acusado de plagio por Blaywer,[339] una publicación electrónica que se edita en el Perú relevando los aspectos coincidentes con otras normas extranjeras como la colombiana y el sustento de la exposición de motivos que habría sido tomada del sitio web monografías que no acredita una solidez de sus contenidos.

Este hecho revela el poco conocimiento del problema informático de nuestros legisladores que deben recurrir a fuentes poco confiables o que carecen del sustento para justificar la eficacia y eficiencia de un proyecto de ley (análisis del costo beneficio), lo que –lamentablemente- en muchas ocasiones ha originado que a los pocos días de expedida se esté modificando la norma, lo cual no contribuye a la seguridad jurídica que tanto se pregona.

El predictamen de la Comisión de Justicia y Derechos Humanos recoge la propuesta de los proyectos Eguren y Salazar e incluye las siguientes tipos penales:

Hurto de Tiempo

El Predictamen de la Comisión de Justicia y Derechos Humanos del Congreso prescribe en su artículo 10 el delito de "hurto de tiempo" cuya conducta central esta definido por el "uso de un sistema de información sin autorización del titular

[339] Vide: www.blawyer.org

o excediéndose del tiempo otorgado por su titular". Sin embargo, esta conducta afecta el principio de ***ultima ratio*** que informa que solo se deben tipificarse conductas que afecten gravemente el sistema de convivencia. Esto es, la conducta denominada "hurto de tiempo" puede ser reprimida por otras ramas del derecho.

Por otro lado, no se identifica cuál sería el bien jurídico que se intenta proteger, ello a pesar que esta conducta se encuentra en el rubro de los delitos contra el patrimonio individual; empero, no se aprecia de qué forma se afecta o menoscaba el patrimonio individual con el acto de disponer o utilizar un sistema informático o tecnología de información sin autorización del titular. Finalmente, sancionarla con una pena máxima de 2 años es una pena simbólica sin efecto preventivo general alguno.

Considero que no es una conducta merecedora de sanción ni que cumple con el principio de intervención mínima del derecho penal y, finalmente, no se aprecia vulneración o puesta en peligro concreto de un bien jurídico como patrimonio o la seguridad de la información informáticamente tratada, por lo que –en mi opinión- debe ser descartada o eliminada del proyecto.

Intrusismo informático

Se sanciona adecuadamente la conducta del hacker o intruso que, sin autorización, accede o interfiere un sistema informático. De esta manera se sanciona el ingreso no autorizado en sí, superando la debilidad del artículo 207º-A que exige la presencia de un elemento subjetivo del tipo.

Sin embargo, esta propuesta incluye en el objeto material las "señales electromagnéticas", la cuales se encuentran amparadas en el tipo de hurto. Además la conducta clásica del intruso o hacker no está asociada a la interceptación de señales electromagnéticas, sino al ingreso a sistemas

informáticos, razón por la que considero que este extremo debería evaluarse de manera objetiva y ver si, efectivamente, es necesario incluirla o, por el contrario, como lo sostenemos, debe excluirse.

Por otro lado, también considero que la pena es simbólica y no resulta proporcional a la lesión del bien jurídico tutelado supraindividual como es la "*seguridad de los datos informáticamente procesados o almacenados*", en virtud de ello, considero que la pena debe incrementarse.

Sabotaje informático

En principio sería conveniente que esta conducta sea definida como los daños informáticos o a sus elementos lógicos, en lugar de utilizar el término "sabotaje" que significa el daño o deterioro de bienes o instalaciones producto de lucha contra patrones, el Estado o en conflictos sociales o políticos.

En primer lugar, en un solo artículo se incluyen diversas conductas los daños informáticos, elaboración y propagación de virus. Por cierto, una técnica legislativa más ordenada aconseja separar los tipos por cada conducta.

En segundo término, la presencia de elementos subjetivos del tipo como enviar o desarrollar programas, páginas web "*con fines ilícitos*" o "*con la finalidad de obtener datos personales*" ocasionan problemas al momento de calificar algunos hechos. El acto de enviar programas nocivos o colgar páginas web a través de las cuales se pueda obtener información personal, empresarial o financiera constituye en sí una puesta en peligro concreto del bien jurídico tutelado. La tipificación debería señalar concretamente la conducta prohibida empleando los verbos correctos como diseñar, enviar, vender, ejecutar, distribuir, dañar, alterar, modificar, eliminar etc. sin agregar un fin ulterior que usualmente complica su correcta tipificación.

En tercer lugar, las conductas de introducir o extraer del territorio nacional programas nocivos no se adecúan a la nueva realidad virtual que nos trae las nuevas tecnologías, en las cual las fronteras o territorios no existen y la difusión de cualquier información o programa en la red se difunde al instante a cualquier parte del mundo. Resulta realmente poco prático.

Adicionalmente, debo indicar que en las propuestas legislativas comentadas falta una correcta tipificación del phising y del hurto de identidad.

7. La criminalidad informática en la Legislación comparada.

A partir de la década de los 80`s, a raíz de las primeras manifestaciones de criminalidad informática o que utiliza medios informáticos, se comenzó a legislar sobre la regulación jurídica de la Internet, los documentos electrónicos y las conductas que afectaban importantes bienes jurídicos. Como podemos ver a continuación, no solo se han producido cambios legislativos producidos a nivel nacional sino que, dada la trascendencia de la nueva criminalidad, las organizaciones internacionales han dictado los lineamientos para sancionar adecuadamente estas conductas. Sin embargo, es de advertir que desde el primer reporte sobre la criminalidad mediante computadoras[340], a mitad de los 70´s, se detectó que la mayoría de estas conductas no se reportaban o ni siquiera eran detectadas.

Diversas organizaciones internacionales, al reconocer el carácter transnacional de la criminalidad por computadoras, recomiendan que la legislación en esta área debe uniformarse. Actualmente, las recomendaciones de los organismos internacionales se encuentran enfocados en las siguientes áreas: i) crímenes contra el patrimonio, ii) violaciones de la intimidad, y iii) los problemas de las leyes procesales[341].

[340] Cfr. Sieber, Ulrich. IUS Informationis. The Internacional Emergence of Criminal Information Law…p. 5.
[341] Cfr. Sieber, Ulrich. IUS Informationis. The Internacional Emergence of Criminal Information Law… p.73 y ss.

El primer esfuerzo internacional para enfrentar el problema de la criminalidad informática fue realizado por la Organización para la Cooperación y Desarrollo Económico (OECD). En 1985 un comité ad hoc recomendó efectuar modificaciones en las legislaciones nacionales que podrían ser considerados como el común denominador de estas conductas.

En 1990, la OECD formulo la "Guía para la Seguridad de los Sistemas de Información" que se centraba en recomendar la implementación de medidas de seguridad para los sistemas de información. Sin embargo, se requiere adecuadas sanciones penales para usos no autorizados de sistemas de información, leyes de extradicción más flexibles y acuerdos de asistencia mutua.

El Consejo de Europa, en 1989, efectuó una declaración mediante la cual adoptó la recomendación elaborada por el Comité de Expertos en Crímenes cometidos por Computadoras, mediante la cual se recomienda a los Estados miembros a tomar en cuenta "La Guía para las legislaciones nacionales", a revisar su legislación o crear una nueva legislación mediante la cual afronte el problema de la nueva criminalidad. "La Guía para las legislaciones nacionales" contiene una "lista minima" con las previsiones legales, en la cual se ha llegado a un consenso sobre los atentados mediante computadoras que deben ser incluidos en las leyes penales y una "lista opcional" de conductas que no alcanzaron consenso.

En la "lista minima" se describen las siguientes conductas:[342]

4. Fraude mediante computadoras. Ingreso, alteración, borrado de datos o programas de computadoras o cualquier interferencia en el procesamiento de datos que produzca perjuicio patrimonial o la pérdida de algún bien.
5. Falsificación. Manipulación del procesamiento de datos que produzca la falsificación de la información.

[342] Cfr. Sieber, Ulrich. IUS Informationis. The Internacional Emergence of Criminal Information Law… p.78.

6. Daños en los datos.
7. Sabotaje informático
8. Acceso no autorizado
9. Interceptación no autorizada
10. Reproducción no autorizada de programas.
11. Reproducción no autorizada de topografía de un network

En la "lista opcional" se incluye las siguientes conductas:

1. Alteración de información.
2. Espionaje.
3. Uso no autorizado del computador.
4. Uso no autorizado de un programa de computador.

En 1990, especialmente en el Congreso de La Habana[343], las Naciones Unidas adoptó una Resolución en el cual insta a los Estados miembros que trabajen intensamente para enfrentar eficazmente contra la criminalidad de computadores, con las reformas legales que contengan previsiones tanto en el derecho sustantivo como en el derecho procesal que otorgue facultades de investigación y conservación de prueba. Que adopten medidas de seguridad que aseguren la protección de la privacidad y de los derechos fundamentales. Elaboración de Códigos de Ética en el uso de las computadoras que debe formar parte de la currícula educativa en la formación de especialista de informática.

Sieber[344] nos advierte que es de especial importancia que la legislación internacional, que regule las conductas ilícitas, se unifique, debido a que los delitos pueden cometerse a distancia cruzando las fronteras ya que si existen diferentes legislaciones pueden crear "paraísos legislativos para el crimen informático".

[343] Cfr. Sieber, Ulrich. IUS Informationis. The Internacional Emergence of Criminal Information Law… p.81.
[344] Cfr. Sieber, Ulrich. IUS Informationis. The Internacional Emergence of Criminal Information Law… p.97.

a. Convenio sobre la Ciberdelincuencia. Budapest. 2001.

El Consejo de Europa, en 2001, en Budapest promulgó su "Convenio sobre la Ciberdelincuencia" en el cual se establecen recomendaciones para que sus países miembros efectúen modificaciones tanto en aspectos de tipificación de delitos como en reglas de procedimiento en los Códigos Nacionales.

En la parte de tipificación de nuevas conductas se divide en dos títulos i) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, ii) Delitos informáticos, iii) Delitos relacionados con el contenido iv) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

i) **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.**

Acceso ilícito. Es "el acceso deliberado e elegítimo a todo o parte de un sistema informático". Esta conducta puede estar vinculada a la violación de medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva.

Interceptación ilícita. Interceptación deliberada e elegítima por medios técnicos de datos informáticos en transmisiones privadas que utilicen el sistema informático.

Ataques a la integridad de datos. Acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

Ataques a la integridad del sistema. Obstaculización grave del funcionamiento de un sistema mediante la introducción, transmisión, alteración o supresión de datos informáticos.

Abuso de dispositivos. Producción, venta, importación, distribución de dispositivos, programas informáticos o contraseñas, códigos de acceso para acceder a sistemas informáticos.

ii) Delitos informáticos.

Falsificación informática. Introducción, alteración o supresión intencional e ilegítima de datos informáticos siempre que puedan ser utilizados como auténticos.

Fraude informático. Introducción, supresión de datos o interferencia en el funcionamiento de un sistema financiero que causen perjuicio patrimonial.

iii) Delitos relacionados con el contenido.

Pornografía infantil. Producción de pornografía infantil con intención de difundirla a través de un sistema informático. Difusión, adquisición o posesión de pornografía infantil a través de un sistema informático.

Adicionalmente, se establecen previsiones para incluir en estas conductas a los cómplices y sancionar la tentativa.

De otro lado, se incluyen medidas legislativas que involucran a las personas jurídicas cuando el autor la haya utilizado para la comisión de los delitos o actúe como representante o miembro de un órgano de administración.

Finalmente, el convenio de Budapest recomienda que estos delitos sean sancionados con penas privativas de libertad, "efectivas, proporcionadas y disuasorias" y penas pecuniarias a las personas jurídicas que sean utilizadas en la comisión de estos delitos.

Es necesario anotar que este convenio incluye medidas procesales que permitan asegurar y conservar los datos informáticos que puedan servir de evidencia, la obtención de los datos informáticos en tiempo real, las interceptaciones de comunicaciones por medios informáticos, confiscación de evidencia almacenada en medios informáticos.

iv) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Propiedad intelectual y derechos afines. Infracciones al derecho de propiedad intelectual previstos en el Tratado OMPI sobre derecho de autor que se cometan por medio de un sistema informático.

Infracciones de los derechos afines cuando se realicen a escala comercial y por medio de un sistema informático.

b. La clasificación de delitos informáticos de la ONU[345]

En el 2005, en el undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal emitió sus recomendaciones sobre los delitos informáticos, en la cual se reconoce que la delincuencia informática implica "la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación; o incluye la utilización incidental de computadoras en la comisión de otros delitos."

[345] www.unodc.org

Tipos de delincuencia informática de acuerdo a la ONU.

- Delitos informáticos que atacan a las propias tecnologías de la información y las comunicaciones, a los servidores y los sitios Web, con virus informáticos de alcance mundial que causan considerables perjuicios a las redes comerciales y de consumidores.
- El vandalismo electrónico y la falsificación profesional.
- El robo o fraude. Ataques de piratería contra bancos o sistemas financieros y fraude mediante transferencias electrónicas de fondos.
- Uso de las computadoras para facilitar una amplia variedad de ventas telefónicas e inversiones fraudulentas mediante prácticas engañosas.
- La "pesca" (phishing) o la inundación de mensajes supuestamente de origen conocido (spamspoofing) u otros sitios legítimos para engañar a los usuarios a fin de que comuniquen datos financieros, datos personales o contraseñas.
- La difusión de material ilícito y nocivo. La Internet se utiliza ahora cada vez más para distribuir material considerado legalmente obsceno en varios países. Otro motivo de preocupación es la pornografía infantil. Desde fines de los años 80, ha venido aumentando su distribución a través de una variedad de redes informáticas, utilizando una variedad de servicios de Internet, incluidos los sitios Web. Una cierta proporción de la distribución de pornografía infantil se ha vinculado a la delincuencia organizada transnacional.
- El uso de la Internet para difundir propaganda y materiales que fomentan el odio y la xenofobia, o que facilite el financiamiento del terrorismo y/o la distribución de propaganda terrorista.

El documento de la ONU pone en relieve los problemas de acopio de material probatorio en investigación y probanza de la delincuencia informática ya que la

mayoría de los datos probatorios son intangibles y transitorios ya que vestigios digitales, que suelen ser volátiles y de vida corta. También se plantean problemas legales en relación con las fronteras y las jurisdicciones. Finalmente, se destaca que en la investigación y el enjuiciamiento de delincuentes informáticos resulta sumamente importante la cooperación internacional.

c. Alemania.

Ley Contra la Criminalidad Informática. 15 de mayo de 1986.

En este país se promulgó tempranamente en 1986 la segunda Ley contra la Criminalidad Económica, que "sirve sobre todo para luchar contra la criminalidad informática (263a, 269, 303a, b) para proteger los pagos realizados por medio de cheque (152a, 266b) y para impedir las inversiones fraudulentas (264a) y el impago de las cotizaciones empresariales a la Seguridad Social (266ª)."[346]

En el Código Penal Alemán (StGB) se encuentran las siguientes normas que sancionan las conductas que utilizan nuevas tecnologías o sistemas informáticos:

1. **Estafa informática (263a).**

   La "estafa informática" en la legislación alemana se configura sobre los elementos de prejuicio patrimonial mediante una manipulación de los datos de un sistema informático con lo cual se supera la limitación que existe en el tradicional delito de estafa que requiere que el engaño se realice sobre una persona física.

   En este caso, la conducta del agente se dirige a burlar, superar las medidas de seguridad o alterar la prefiguración del programa o sistema informático para obtener un beneficio patrimonial indebido.

[346] Cfr. Roxin, Claus. *Código Penal alemán*. StGB. Ed. Marcial Pons, 2000, p.17.

Este tipo penal exige que el beneficio patrimonial se obtenga o provenga de "una errónea configuración del programa, del uso incorrecto o incompletos, uso no autorizado de datos o de intervención no autorizada.

El articulo 263a del Código Penal Alemán[347] cubrió la laguna de punibilidad que existía en el delito de estafa que no podia sancionar las manipulaciones informáticas como una maniobra fraudulenta. Sin embargo, queda a discusión si esta modificación tambien comprende al uso de tarjetas en los cajeros automaticos ya que anteriormente la jurisprudencia alemana sancionaba estas conductas con el tipo penal de robo.

2. Falsificación de datos probatorios (269)[348]

Se sanciona la alteración o modificación de datos o el uso de datos modificados con el objeto de engañar en el tráfico jurídico. La alteración o falsificación de los datos tienen relevancia penal cuando éstos sean "datos probatorios relevantes".

3. Alteración de datos (303a)

La conducta está referida a modificar o inutilizar o borrar ilegalmente datos que se encuentran almacenados o transmitidos en un sistema informático[349].

[347] Information Technology… Germany Computer Crimes p. 219.
[348] De acuerdo a Möhrenschlager "el artículo 269 busca cubrir el vacío respecto a la portección del documento electrónico como evidencia en Information Technology… Germany Computer Crimes p. 220.
[349] Information Technology… Germany Computer Crimes p. 221.

4. Sabotaje informático (303b).

Se sanciona la destrucción de datos o los soportes de datos.
La norma alemana establece que los datos objeto de protección deben ser "de especial importancia para una industria, empresa ajena o autoridad".

De acuerdo al profesor Möhrenschaler[350] No existe una norma que sancione la hacker o los accesos ilegales.

d. Estados Unidos de Norteamérica.

The Computer Fraud and Abuse Act 1994.

En Estados Unidos[351] la legislación relacionada con el uso de las computadoras hay tres etapas; la primera, se inició por la gran cantidad de informacion personal almacenada en computadoras y en las que se dictó la primera ley de reporte de crédito de 1970, la ley de protección de la intimidad de 1974 y leyes de protección de información privada; la segunda, entre 1975 y 1978, se dictan leyes sobre la criminalidad por computadoras que prohíben el acceso o uso no autorizado de computadoras y la tercera que incluye a los programas de computadoras en la protección de los derechos de autor o la propiedad intelectual.

La ley de 1986 sanciona delitos que involucra intereses federales del uso de computadoras. La mayoría de los delitos de computadoras se refieren a robos y los fraudes de computadoras en las cuales la legislación norteamericana tiene similares dificultades que existen en otros países con las tradicionales figuras

[350] Information Technology… Germany Nacional Report…p. 215.
[351] Information Technology… Computer Crime and Other Crimes against Information Technology in The United States. National Report by Prof. Edward M. Wise. p. 517.

delictivas contra el patrimonio[352]. El típico fraude que consiste en la introducción de información en computadoras con el propósito de obtener algún beneficio económico puede ser fácilmente sancionado como robos o, si se utiliza medios de comunicaciòn inter estatales, como fraude de correos.

En el aspecto penal resulta relevante el Acta Federal de Abuso Computacional de 1994 que modificó al Acta de Fraude y Abuso Computacional de 1986. Esta ley federal tipifica diversas conductas que utilizan o se valen de un sistema informático que busca prohibir el acceso ilegal a sistemas informáticos, la propagación de virus informáticos y el fraude informático.

1. Acceso no autorizado o excediendo la autorización cuando se:
   1.1. Obtiene información concerniente a la seguridad nacional o relaciones internacionales mediante
   1.2. Consigue información financiera o accede al sistema informático de una institución financiera o del Gobierno Federal.
2. Acceso no autorizado al sistema informático del Gobierno de Estados Unidos o sus agencias.
3. Acceso no autorizado con intención de defraudar.
4. Difusión de virus que ocasionen daños a computadoras que pertenecen a entidades financieras, que se utilicen en comunicaciones o comercio interestatal o internacional o que pertenezcan al gobierno de Estados Unidos.
5. El uso del sistema informático para extorsionar.

[352] Information Technology… United States. National Report... p. 520.

El fraude por correo (*mail Fraud)* de la legislación norteamericana.

Asimismo, es interesante subrayar que en Estados Unidos se sancionaba en la Sección 1341 del Título 18, como delito federal, algunas conductas defraudatorias o de estafa cuando utilizaban el correo nacional como medio para cometer estos delitos, con prisión hasta 5 años y multa. En la Sección 1343 del Título 18 se castiga hasta con 20 años el fraude o estafa cometido por medio de la televisión, radio o cualquier comunicación interestatal

e. Gran Bretaña. *The computer Misuse Act.* 1990 de 29 de julio de 1990.[353]

En 1990 se dictó una "Ley sobre el mal uso de las computadoras" el cual constituyó en "el cambio más importante en la legislación"[354] que tipifica conductas que utiliza la informática la cual fue modificada en 2006 y prevé penas de hasta 10 años y multa.

Conforme se precisa en su exposición de motivos se pone acento en el carácter "indebido" o "sin autorización" del acceso a un sistema informático o modificación de datos informatizados.

La legislación británica básicamente tipifica las siguientes conductas:

1. Acceso no autorizado a un sistema informático para obtener la instalación de un programa en computadora o con la intención de cometer o facilitar otros delitos. Se refiere a un acceso sin autorización cuando se ingresa o

[353] www.legislation.gov.uk/ukpga/1990/18
[354] Information Technology… Computer Crimes... United Kingdom Nacional Report by Prof. Dr. Martin Wasik. p. 215.

acceda a cualquier programa o datos sin el consentimiento de la persona que tenga las facultades para darlas[355].

2. Manipulación no autorizada para poner en peligro o perjudicar el funcionamiento de una computadora. De esta manera se crea un rango amplio de conductas que cubre la alteración o borrado de cualquier programa o información que se encuentra en una computadora. Empero, según Wasik[356] en esta sección se debería incluir también la introducción intencional de virus informáticos y cuando se altere o modifique el contenido de una computadora

3. Suministrar u obtener de artículos a través la computadora.

f. Reino de España.

En la reforma de 1995 del Código Penal Español se introduce conductas referidas a los delitos informáticos. Según Gutierrez Francés[357] los pilares básicos del código español se encuentran en el Código de 1848, por lo que es fácil de advertir las deficiencias de aquella legislación con las nuevas manifestaciones de la delincuencia y solo desde el proyecto de 1992 refleja cierta preocupación por la modernización del derecho penal en este campo como debería ser.

De acuerdo a la profesora española,[358] el Código Penal español solo protege la información. El extraordinario desarrollo de la información y su incremento de su valor económico ocasionado por las tecnologías no se ha reflejado en la legislación.

[355] Information Technology… United Kingdom Nacional Report by Prof. Dr. Martin Wasik. p. 494.
[356] Information Technology… United Kingdom Nacional Report by Prof. Dr. Martin Wasik. p. 497.

[357] Information Technology… Computer Crime and Other Crimes against Information Technology in Spain. National Report by Dra. María Luz Gutierrez Francés. p. 434 y ss.
[358] Information Technology… Spain. National Report by Dra. María Luz Gutierrez Francés. p. 436 y ss.

La violación de secretos de estado o privados que se encuentra en el Código Penal puede aplicarse a aquellos que están procesados o almacenados en computadoras. Sin embargo, los artículos respecto a la infidelidad de la custodia de documentos y la violación de la correspondencia no pueden incluir la información computarizada, pues solo se refieren a correspondencia como papeles escritos.

1. **Descubrimiento y revelación de secretos (art. 197 y siguientes).**

   En los delitos contra la intimidad[359] se amplían los tipos penales con el propósito de incluir las nuevas formas de comunicación, almacenamiento o procesamiento de datos. De esta manera, será posible el apoderamiento de correos electrónicos o de cualquier otra señal de comunicación.

   También se incluye, en el artículo 197.2, como objeto de protección los datos personales registrados en soportes informáticos, electrónicos o telemáticos. De acuerdo a Vives[360], las conductas aquí tipificados "se proyectan sobre ficheros o soportes informáticos, electrónicos o telemáticos."

2. **Delitos contra el honor (art. 211)**

   Se considera que la publicidad exigida en la injuria grave es factible realizarla por cualquier medio informativo que propague la calumnia o injuria.

3. **Delitos contra el patrimonio. Robos (art. 238).**

   Los robos con fuerza en las cosas mediante el uso de llaves falsas. En el concepto de "llaves falsas" se encuentran las tarjetas magnéticas o perforadas. De esta manera, el robo -es decir el apoderamiento de una cosa

[359] Vives resalta el hecho que aunque este rubro debería denominarse "delitos contra la intimidad de las personas mediante el uso de la informática y de las comunicaciones" el bien jurídico "intimidad" sigue siendo el mismo. Ob. Cit. p. 258.
[360] Vives. Ob. Cit. p.259. (AGREGAR)

mueble ajena- se realiza mediante una tarjeta electrónica o magnética que permita el acceso al bien ajeno.

4. **Estafas Informáticas 248.2.**

   Se tipifica las estafas con ánimo de lucro valiéndose de alguna "manipulación informática o artificio semejante." De esta manera, siguiendo la fórmula alemana, se supera el concepto tradicional de engaño como elemento central del delito de estafa en la cual solo se puede realizar contra una persona física. En este caso, se establece que las manipulaciones o alteraciones de sistemas informáticos que resulten idóneos para obtener una "transferencia no consentida" de fondos.

   Gutierrez Francés[361] nos informa que el proyecto de 1992 adoptó la posicion de la mayoría de la doctrina asignando dos preceptos: del fraude por computadoras a través de las manipulaciones de computadoras y el uso indebido de las tarjetas magneticas son resueltas con el delito de robo, ya que estas se homologan al concepto de llaves.

5. **De las defraudaciones de fluido eléctrico y análogas (art. 255).**

   Se considera como objeto material de esta conducta las energías o cualquier otro elemento con valor económico y en las conductas se comprende las alteraciones o manipulación en los aparatos que controlan el consumo de estos elementos.

6. **Uso de terminales de comunicación (art. 256).**

   Las terminales de comunicación también se encuentran protegidas de su uso abusivo o sin consentimiento del titular. Entre estas terminales también se consideran a los que realizan comunicaciones mediante sistemas informáticos.

[361] Information Technology… Spain. National Report by Dra. María Luz Gutierrez Francés. p. 436.

7. **Daños (art. 264).**

   En el capítulo de daños a la propiedad ajena se comprende, como objeto material, los elementos inmateriales que forman parte de un sistema informático como los "programas o documentos electrónicos".

8. **Delitos relativos a la propiedad intelectual (art. 270).**

   Entre los objetos de protección se comprende a las obras que se encuentran fijadas en "cualquier tipo de soporte o comunicada a través de cualquier medio".

9. **Delitos relativos al mercado y a los consumidores (art. 278)**

   Se protegen los secreton de la empresa que se encuentren contenidos en cualquier medio incluido los documentos electrónicos, comunicaciones o soportes informáticos.

10. **Tenencia o fabricación de elementos para falsificar (art. 400)**

    Se sanciona la fabricación o tenencia de programas de ordenador o aparatos que permitan las falsificaciones.

g. Chile.

Ley relativa de delitos informáticos. Ley Nº 19223 de 28 de mayo de 1993.

Chile fue el primer país latinoamericano en promulgar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos:

1. **Destrucción de datos.** Se sanciona la destrucción de datos. En realidad esta conducta se confunde con la tipificada en el artículo 3 de esta ley que sanciona los daños a los datos informáticos.

2. **Obstaculizar el funcionamiento de un sistema informático**.

   La conducta se agrava cuando se ocasione daños en los datos.

3. **Interceptación o acceso a un sistema informático**. Aquí no se sanciona la conducta e hacker o intruso, sino cuando se ingresa indebidamente con el propósito de apoderarse, usar o conocer la información de un sistema informático.

4. **Dañar o destruir la data.** Se refiere a la inutilización o deterioro de los datos contenidos en un sistema informático.

5. **Difundir datos.** Se sanciona la conducta de difundir información confidencial. La conducta se agrava en razón a la calidad del sujeto activo cuando éste es el responsable de la administración del sistema.

La ley chilena exige la existencia de un elemento sujetivo del tipo al indicar que las conductas descritas en la Ley relativa a Delitos Informáticos se realicen con el "ánimo" o actúen "maliciosamente". Esta exigencia puede causar problemas probatorios al momento de perseguir estas conductas.

De acuerdo a Kunsemuller[362] la ley chilena tiene tres propositos:

[362] Information Technology. Chile Computer Crimes and other Crimes against Information Technology in Chile. National Report by Prof. Carlos Kunsemuller. p. 133.

1. El uso de los procesos automatizados de data para perpretar delitos tipificados en el Código Penal se considera una circunstancia agravante.
2. Impedir u obstaculizar el proceso automatizado de datos.
3. Programar o utilizar un sistema informático para obtener información.

h. Colombia[363].

Ley Nº 1273 del 05 de enero de 2009.

Desde 2009, Colombia tiene una muy completa y bien lograda ley que incorporó al Código Penal el Título VII BIS De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, en el cual crea un nuevo bien jurídico denominado: "De la Protección de la información y de los datos".

Esta ley sanciona el acceso indebido, la obstaculización ilegítima de un sistema informático, interceptación de datos informáticos, el daño informático, la difusión de virus informáticos y la creación de sitios web falsos.

1. **Acceso abusivo a un sistema informático.** Sanciona las siguientes conductas: i) el acceso ilegal, esto es, sin autorización a un sistema informático lo cual implica sancionar la conducta del intruso o el hacker quien simplemente ingresa a un sistema informático sin que se le exija o ii) continuar dentro del sistema a pesar del requerimiento de quien tenga la capacidad para hacerlo lo cual implica que el acceso inicial pudo ser legítimo pero se torna indebido cuando se le requiere que abandone el sistema.

[363] www.secretariasenado.gov.co/senado/basedoc/ley/1273

2. **Obstaculización ilegítima del sistema informático o red de comunicación.** La conducta central es impedir, obstaculizar el funcionamiento o acceso con lo cual se sanciona, por ejemplo, la saturación del envío masivo de correos a la bandeja de entrada o bloquear el acceso de una página web por enviar gran cantidad de spam. Nótese que la ley considera que el objeto material también puede ser la red de telecomunicaciones que puede ser operada por un sistema informático o no.

3. **Interceptación de datos informáticos.** Se sanciona cualquier forma de acceder u obtener datos que se encuentren en un sistema informático o hayan sido transmitidos por éste. De esta manera se protege cualquier tipo de información que haya sido enviada por cualquier medio electrónico o que se encuentre almacenada en un sistema informático.

4. **Daño informático.** Se sanciona, con un vocablo más adecuado que el "sabotaje" utilizado en otras legislaciones, la destrucción o alteración de los datos informáticos o de los componentes lógicos.

5. **Uso de software malicioso.** La ley colombiana definía a los conocidos "virus informáticos" que constituyen programas que causan daños en la información o permiten obtener datos que contiene el sistema. Este tipo penal sanciona el que se comercialice, distribuya, introduzca al territorio nacional cualquiera de este tipo de programas de computación. Sin embargo, hay que tener en cuenta que la difusión de estos programas se realizan por la propia red, por lo que no queda muy claro la conducta descrita como "introducir o extraer" del territorio nacional, ya que en muchos casos por la propia característica del sistema informático y la

Internet las fronteras entre los países resulta un concepto que no se ajusta a la realidad informática. Hubiera sido preferible indicar como conducta típica "difundir o transmitir" por la red a cualquier sistema informático.

6. **Violación de datos personales.** Se refiere a que se obtenga, difunda, modifique códigos o datos personales que se encuentren en bases de datos de sistemas informáticos.

7. **Suplantación de sitios web.** Se sanciona aquí a la conocida conducta de "phishing"; esto es, enviar una página web falsa de un banco u otra entidad confiable con el objeto de engañar a los usuarios para que éstos proporcionen sus datos personales como su clave de acceso a sus cuentas.

Se establecen como conductas agravadas las siguientes:

1. **Por el objeto material.**

   Sistema informático o de comunicaciones estatales o del sector financiero.

2. **Por la calidad de sujeto activo.**

   Servidor público en ejercicio de sus funciones.
   Responsable de la administración o control de la información.

3. **Por el móvil.**

   Fines terroristas
   Obtener provecho

4. **Otras circunstancias.**

   Utilizar como instrumento a un tercero

   Revelar la información obtenida

El Capítulo II de la norma colombiana sanciona los fraudes y transferencias no consentidas de fondos.

1. **Hurto por medios informáticos.** Se sanciona el apoderamiento de fondos mediante la manipulación de un sistema informático, telemático u otro semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización.

2. **Transferencia no consentida de activos.** Se sanciona la manipulación informática para obtener transferencias no consentida de activos y la posesión, distribución o elaboración de programas de computación que faciliten o permitan estas transferencias ilegales de fondos.

Conducta agravada.

Se agrava la conducta si el perjuicio fuere superior a 200 salarios mínimos mensuales.

8. ANÁLISIS Y COMENTARIOS SOBRE LOS RESULTADOS DE LA INVESTIGACIÓN.

A. Síntesis del trabajo de campo

Para el desarrollo del trabajo de campo o investigación tuvimos una serie de dificultades que no contemplamos al momento de desarrollar nuestro proyecto, en la medida que era algo no previsible y que dificultaron realizar nuestra labor, sobre todo en el acopio de las muestras.

Básicamente, nos encontramos con dificultades para obtener las entrevistas a los Magistrados, abogados y los justiciables. En el primer caso estaban referidos principalmente a su carga laboral y limitado horario de atención al público, además de la propia reticencia que nos manifestaron muchos de ellos para someterse a la entrevista, situación que también se apreció con los abogados, quienes aduciendo estar ocupados se negaban a brindarnos la entrevista o desarrollar las encuestas. Realmente, consideramos que esto se debe a una suerte de temor de los Magistrados y Abogados por la posibilidad de quedar "mal parados" ante estas entrevistas y encuestas, a pesar que se les reiteraba que los resultados iban a ser reservados, así como sus respectivas identidades (anónimos).

Por todo ello, debemos señalar que los resultados que a continuación analizaremos se obtuvieron sobre la siguiente muestra: 20 Magistrados, 10 abogados y 05 efectivos de la PNP de la DIVANDAT; así como un total de 30 expedientes, que consideramos una muestra válida para el desarrollo del presente trabajo.

En principio, debemos mencionar que la criminalidad informática es uno de los principales aspectos de la seguridad ciudadana, como se confirma con la estadística de la evolución de la criminalidad informática proporcionados por la DIVANDAT-PNP y el Ministerio Público:

Incidencia delitos relacionados con la Informática 2009

DELITO	**TOTAL**
Hurto de fondos	523
Pornografía infantil	65
Delitos informáticos	125
Delitos especiales	223
Total	**936**

Incidencia delitos relacionados con la Informática 2010

DELITO	TOTAL
Delito contra la vida, CS	1
Coacción	64
Violación sexual	11
Actos contra pudor	28
Trata de personas	3
Secreto comunicaciones	8
Violación intimidad	14
Pornografía infantil	90
Hurto de fondos	384
Estafa	45
Extorsión	66
Delitos informáticos	161
Contra la fe pública	24
Otros	35
Total	**934**

Incidencia delitos relacionados con la Informática 2011[364]

DELITO	TOTAL
Delito contra la vida, CS	2
Coacción	60
Violación sexual	1
Actos contra pudor	16
Trata de personas	1
Secreto comunicaciones	11
Violación intimidad	7
Pornografía infantil	121
Hurto de fondos	526
Estafa	42
Extorsión	67
Delitos informáticos	156
Contra la fe pública	25
Otros	41
Total	**1076**

A nivel del **Ministerio Público**[365] tenemos la siguiente data:

En el año 2009 tuvieron un ingreso de 307,233 denuncias, de las cuales fueron atendidas 251,503 (83.5%), quedando pendientes de resolver 32,130 (16.5%) del total ingresadas. Los distritos judiciales que concentraron la mayor cantidad de denuncias ingresadas fueron Lima con 41,847 (15.0%), seguida de Arequipa con 15,414 (7.9%) y Lambayeque con 55,730 (6.9%) denuncias.

Entre los delitos genéricos que alcanzan el mayor número durante el año 2009, se encuentran los delitos contra el patrimonio, lo que representó el 32.5 % (20,631) del total de casos por delitos ingresados, donde el delito de hurto registró 4,994 casos

[364] Información brindada por la DIVANDAT-PNP hasta el mes de setiembre de 2011.
[365] Todos los datos obtenidos y que se hacen mención en esta investigación están en la web del Ministerio Público: http://www.mpfn.gob.pe/estadistica/anuario_est_2009.pdf

lo que representó el 24.5% de los casos de delitos contra el patrimonio, aunque es de señalar que no se especifica el porcentaje de casos en que el hurto se realizó a través de usos de medios informáticos. Sí se indica, en cambio, que en dicho año existieron 96 casos de Delitos informáticos que representan el 0.47% del total comentado.

En el año 2010, las fiscalías provinciales penales y mixtas de los distritos judiciales con Antiguo Código de Procedimientos Penales tuvieron un ingreso de 157,566 denuncias, de las cuales fueron atendidas 151,451 (96.1%), quedando pendientes de resolver 6,115 (3.9%) denuncias del total de ingresadas. Los Distritos Judiciales que concentraron la mayor cantidad de denuncias ingresadas fueron Lima con 47,407 (30.1%), seguida de Junín con 14,105 (9.0%), Lima Norte con 14,011 (8.9%), Lima Sur con 11,255 (7.1%) y Callao con 10,890 (6.9%) denuncias.

Entre los delitos genéricos que alcanzaron el mayor número durante el año 2010, se encuentran los delitos contra el patrimonio, lo que representó el 32.5 % (25,826) del total de casos por delitos ingresados, donde el delito de hurto registró 6,037 casos lo que representó el 23.4% de los casos de delitos contra el patrimonio. Empero, insistimos, en esta data no se especifica la modalidad del hurto, es decir, si se ejecutó con el uso de medios tecnológicos. En cuanto a los Delitos informáticos, este también se incrementó en relación al año anterior y se tiene 154 casos, que representa el 0.6% del total comentado.

De una simple evaluación de estos datos, no podemos dejar de expresar nuestra preocupación por la gran incidencia que están teniendo estos ilícitos penales, destacando los delitos de hurto de fondos, pornografía infantil y delitos informáticos. Estos datos no hacen más que confirmar la tendencia expresada ya desde hace algunos años atrás, en que se sostenía que los mayores casos de fraude informático están constituidos por el abuso de cajeros automáticos de Bancos, y

por lo tanto por la criminalidad menor, donde además casi siempre son autores personas ajenas a la empresa. Con buen instinto, Kaiser pronosticaba que "con el creciente empleo de sistemas procesadores de datos, en el futuro la cuota de autores externos (debería) incrementarse"; como consecuencia de la constitución de formas delictivas técnicamente cada vez más refinadas, al mismo tiempo, sería probable un desplazamiento del círculo de víctimas de los operadores del sistema a los usuarios del sistema, así como la aparición de una criminalidad informática transnacional.[366]

En el campo del homebanking, los esfuerzos se dirigen a afrontar los riesgos para la banca y el usuario a través de una identificación automatizada en la recepción telefónica de encargos individuales y de la grabación –autorizada por el cliente- de estas conversaciones. Igualmente la industria de los chips intenta asegurar las tarjetas de chip contra falsificaciones, tomando medidas estandarizadas contra un análisis del contenido del chip; p. ej. cubriéndolo con una capa de seguridad, cuya separación borre los datos relevantes para la seguridad.

Sin embargo, tal como muestran las posibilidades técnicas para evitar los fraudes en las cuentas en el campo de la telefonía celular [móvil], tienen que considerarse plenamente los intereses divergentes de la protección de datos del lado de los consumidores y la prueba de autenticidad del lado de los usuarios (de los teléfonos celulares) con la finalidad de garantizar la prueba de cálculo de la tarifa. Empero, en resumen, la interconexión global posibilitada por la Internet trae consigo, según una estimación de la propia policía, una nueva calidad de criminalidad que afecta numerosos ámbitos de la vida y de la economía,[367] tal como se refleja en los datos estadísticos comentados, en la que se puede apreciar que la informática ha ingresado en todos los niveles de los ilícitos penales que afectan diferentes bienes

[366] Cfr. Tiedemann, Klaus; *Derecho Penal y nuevas formas de criminalidad…* p.86.
[367] Cfr. Tiedemann, Klaus; *Derecho Penal y nuevas formas de criminalidad…* pp.92-93.

jurídicos (la vida, la libertad, por ejemplo), y ya no solo los exclusivamente patrimoniales; por lo que se justifica encontrar soluciones también desde la perspectiva del Derecho penal.

1. MUESTRA ESTADÍSTICA (ALEATORIA) ANALIZADA

a. **Denuncias policiales:**[368] **936 (2009), 934 (2010) 1076 (2011)**
b. **Formalización de denuncia fiscal: 45%**
c. **Procesos penales en trámite: 10%**

En principio, hemos de mencionar que los porcentajes aquí señalados son respecto al promedio de número de denuncias, es decir, que un aproximado de un poco menos de la mitad de denuncias fueron admitidos por el Ministerio Público, que entendió que existían suficientes elementos probatorios iniciales para formular la denuncia; empero, sólo se encontraban en trámite de investigación judicial un promedio de 10%. Ello implica que de un promedio de 950 denuncias relacionadas con el uso de medios informáticos, sólo estaban procesados penalmente un aproximado de 95 procesos, razón por lo que encontrar en los distintos juzgados penales un proceso en trámite de Delito informático (así, como tal) es bastante raro, no es algo común. Distinto son los casos en que se utilizan medios informáticos para la comisión de distintos delitos, como los cometidos contra el patrimonio que sí están como Hurtos o Estafas.

En las entrevistas tenidas con los oficiales de la DIVANDAT-PNP, básicamente nos manifestaron que el primer problema a tener en cuenta en la investigación y posterior juzgamiento es que los propios agraviados no formulan la denuncia correspondiente y, por consiguiente, tampoco proporcionan los elementos

[368] Los datos que seguidamente analizaremos, fueron proporcionados por la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI – PNP, y los contrastamos con lo que maneja el Ministerio Público y lo que pudimos obtener al apersonarnos a los distintos juzgados penales de Lima.

probatorios necesarios, sobre todo en el tema patrimonial en que se necesita acreditar la preexistencia de lo hurtado o robado, y es que –según nos informaron- la mayoría de los afectados con el uso de la tecnología son entidades bancarias y financieras, quienes tendrían sobradas razones para no hacer público tales actos, pues perderían mucha credibilidad y el riesgo de que pudiera producirse una corrida en el retiro de sus afiliados si se supiera la magnitud del problema, además de que cuentan con el respectivo seguro y cada vez realizan mejoras en sus sistemas de seguridad.

Del mismo modo, las entidades telefónicas tampoco proporcionan –de manera oportuna y con la inmediatez que se requiere- la información referida a la identificación del IP, a fin de proceder a la intervención policial. Realmente, este es un importante escollo que no permite avanzar ni en la denuncia ni en el procesamiento de estos delitos, por lo que se hace necesario se dicte las normas pertinentes para que estos actos no queden impunes.

2. DELITO CON EL QUE SE RELACIONA

a. Extorsión: 66 (2010) 67 (2011)
b. Coacción: 64 (2010) 60 (2011)
c. Contra el patrimonio:
   Hurto: 523 (2009), 384 (2010), 526 (2011)
   Apropiación ilícita
   Estafa: 45 (2010) 42 (2011)
   Administración de persona jurídica
d. Delitos informáticos: 125 (2009), 161 (2010), 156 (2011)
e. Contra el honor
f. Violación secreto de las comunicaciones: 8 (2010) 11 (2011)
g. Violación a la intimidad: 14 (2010) 7 (2011)

h. Contra la libertad sexual: 39 (2010) 17 (2011)
i. Pornografía infantil: 65 (2009), 90 (2010), 121 (2011)
j. Trata de personas: 3 (2010) 1 (2011)
k. Fe Pública: 24 (2010) 25 (2011)
l. Delitos especiales: [369] 223 (2009)
m. Otros: 35 (2010)[370] 41 (2011)

En la data están incluidos los casos de Violación sexual y actos contra el pudor en agravio de menor de edad, aunque es de señalar que nuestros entrevistados policiales no supieron explicitar de qué manera se utilizó la informática para practicar el acto sexual, según la descripción estricta del tipo penal. Sin embargo, del análisis del atestado policial, en nuestra opinión existe una confusión en la investigación y en la ubicación de la data, pues se confunde como elemento probatorio (que es el vídeo) con el delito en sí mismo (acto sexual); por lo que debe entenderse que estos vídeos son solo elementos de prueba para la comisión de los tipos penales de violación o actos contra el pudor, en otras palabras, es el propio agente o su cómplice quien registra el acto sexual para luego subirla en la red o venderla en el mercado negro nacional o internacional como pornografía, incluso infantil (pedofilia) que es a lo que realmente se refieren estos datos.

Igual sucede con la Trata de blancas, en que la Internet es el medio utilizado para contactarse con las víctimas que generalmente son menores de edad y de procedencia de zonas alejadas del país, razón por la que los datos no reflejan esta grave realidad, no solo por la lejanía, sino porque incluso los padres reciben dinero adelantado por los supuestos trabajos de sus hijas y desconocen las reales

[369] Datos proporcionados por la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI – PNP. Es de precisar que en este rubro se encontraban comprendidos los otros delitos que a partir del 2010 ya aparecen disgregados.
[370] En los datos que se anotan, hay uno por homicidio, aunque no se precisa sus circunstancias, ocurrido en febrero 2010. Igualmente, en julio y agosto de 2011 hubo un caso en cada mes referido a delitos contra la Vida, aunque no se precisa circunstancias, pero –según los comentarios de nuestros entrevistados- se trataría de casos en que el trato para la comisión del homicidio se hizo por la web.

condiciones en que son tratadas dichas menores. De los datos también se observa que es innegable el incremento de la pornografía, principalmente relacionado con menores de edad, ello en razón de que existe un mercado ávido por estos vídeos. Del mismo modo, es de considerar que los casos de Extorsión y Coacción, así como delitos contra la Intimidad, están relacionados también con la tenencia de cierta información contenida en medio informático en perjuicio de la víctima, muchas veces el agente de estos ilícitos es una ex pareja que pretende aprovecharse de esta circunstancia y pretende difundir ilícitamente tales imágenes en las que, inicialmente, pudo haberse registrado con el consentimiento de la agraviada, en el entendido de que ello quedaría en el ámbito privado, personal; empero, luego pretende ser utilizado de modo ilícito a través de la amenaza de su difusión no consentida.

Como ya lo comentábamos al interior de esta investigación, estos datos nos confirman que los casos de Hurto y Estafa son en los que más se utilizan los medios informáticos para la comisión de estos ilícitos. Empero, es de señalar que del análisis de los casos que pudimos analizar, y en nuestra opinión, consideramos que en un importante número hay error en la subsunción de los hechos. Recordemos que en la Estafa el delito se comete por el engaño-error-desprendimiento patrimonial-perjuicio económico en que incurre el agraviado. Es el típico caso en que se utilice una tarjeta clonada o falsa en un establecimiento comercial, empero, los mismos fueron considerados como Hurto telemático, por lo que aquí consideramos que hay un grave error de tipificación.

3. NÚMERO DE PROCESADOS

a. **1: 30%**
b. **2 – 3: 20%**
c. **3 – 5: 50%**

d. Más de 5

Bueno, en principio, es necesario precisar que en el delito de pornografía infantil, generalmente está implicada directamente una sola persona o al menos no se sabe de otras; que luego vende el vídeo que graba del acto sexual tenido con una menor de edad. En los casos que pudimos analizar (en un 30%) solo se encontraban denunciados/procesados una sola persona, quienes actuaban a través de una cabina de internet en donde captaba a sus víctimas. En los casos de Extorsión por difusión de vídeo íntimo, la mayoría de las veces el agente es una sola persona, rara vez involucra a otra.

En algunos casos (20%), se detuvo a una sola persona, pero se implicó a otros como no habidos, integrantes de una organización criminal, razón por la que también se les denunció por Asociación ilícita para delinquir. Igual ocurre en los casos que estaban siendo denunciados/procesados entre 3-5 personas (50%).

En los delitos contra el patrimonio (Hurto y Estafa) se les implicaba a algunos ser: líderes o cabecillas, a otros captadores de cuentas de ahorro, tarjetas de débito y claves, otros eran titulares de cuentas receptoras, etc. En los delitos de Pornografía se pudo apreciar que a algunos se les imputaba ser líderes, mujeres en la captación, otros para la distribución y/o comercialización de los vídeos; etc. En otras palabras, verdaderas organizaciones criminales en las que claramente se podían apreciar los diferentes roles que asumían sus integrantes. Igual ocurre en la Trata de blancas.

4. AGRAVIADOS

a. Institución pública (Ministerios, PJ, Congreso, TC, Municipalidades, SBS, PNP, EP, FAP, etc.): 20%

b. Instituciones privadas (bancos, financieras, empresas…): 80%

c. Personas naturales: 70%

Es de precisar, en principio, que en algunos casos (70%), la parte agraviada puede ser un banco/financiera y una persona natural a la vez, titulares de las cuentas afectadas, razón que justifica la casi repitencia de los porcentajes, y en un 10% en que solo el banco aparece como directamente agraviado.

Los datos nos dan una idea de que, al menos en nuestro país, los agraviados de los delitos en que se utilizan medios informáticos y los propiamente delitos informáticos, son instituciones o empresas privadas (para los delitos de Hurto telemático y Estafa, a incluso intromisión), mientras que las entidades estatales son los menos, aunque no por eso menos importante, puesto que ya Anonymus, por ejemplo, nos demostró que el Poder Judicial, la PNP, entre otros, son altamente vulnerables, a pesar de la información sensible que manejan, razón por la que se deben realizar mayores esfuerzos por mejorar los sistema de seguridad.

5. MONTO AFECTADO

a.	**Menor de 10,000:**	**40%**
b.	**De 10,100 a 50,000:**	**30%**
c.	**De 50,100 a 100,000:**	**20%**
d.	**De 100,100 a 500,000:**	**10%**
e.	**De 500,100 a 1`000,000**	**0%**
f.	**Mayor de 1`000,000**	**0%**

Bueno, aquí vemos los casos que de manera directa han estado afectados el patrimonio de las personas –naturales o jurídicas. De la información presentada, podemos apreciar que en la mayoría de los casos (70%) se refiere a montos

menores a los S/.10,000 realizados con actos de compra con tarjeta de créditos falsos o clonados, o incluso hurtos de montos menores a los S/.2,000 nuevos soles, relacionados directamente con los límites establecidos en los cajeros automáticos.

Ello podría explicar el porqué los agraviados no toman mayor responsabilidad en el seguimiento de la denuncia, pues no aprecian la magnitud de los montos que realmente pueden estar en juego. Nos explicamos, tal vez si vemos de manera individual claro que el daño no es mucho, pero si comprendemos que estas organizaciones criminales afectan a decenas de personas, comprenderemos que se afecta significativamente el patrimonio individual y, sobre todo, la credibilidad en el sistema financiero-bancario.

Principales conductas no tipificadas

Lo siguiente es el resumen de las entrevistas tenidas con los oficiales de la DIVANDAT-PNP, Magistrados del Poder Judicial y Ministerio Público, así como de los especialistas en el tema materia de investigación, es el resultado de sus respectivas experiencias y que lo exponemos de este modo en la medida de que no pueden ser cuantificables.

Igualmente, es necesario precisar que estas conductas están relacionadas con el uso de la informática y la tecnología de la comunicación mediante las cuales se acceden a la computadora, base de datos o se obtiene los datos de información bancaria o financiera del agraviado.

Es de notar que estas conductas no constituyen un ilícito en sí ni necesariamente lesionan un bien jurídico tutelado en la norma penal, sino que pueden ser actos preparatorios de otras conductas delictivas como obtener la información personal, bancaria o financiera con la cual pueden efectuar transferencias no autorizadas de

fondos. Sin embargo, deben ser tipificados por poner en peligro algunos bienes jurídicos.

En efecto, recordemos que mediante el phising, vishing o el pharming se obtienen los datos de la cuenta bancaria y la clave secreta; empero, con esta acción no se consigue en sí beneficio económico alguno, sino que posteriormente esta información le servirá para efectuar la conducta prevista en el artículo 186 inciso 3, Hurto telemático, al acceder a la cuenta de la víctima y transferir sus fondos a cuentas de terceros, por lo que insistimos debe incluirse en el catálogo de ilícitos penales.

B. Contrastación de hipótesis

Contrastamos los resultados obtenidos del análisis y procesamiento de datos con el problema formulado al inicio de la investigación, a fin de demostrar la validez o no de nuestra hipótesis, así como de la efectividad de las sugerencias que realicemos para la solución del problema en los distritos judiciales mencionados.

En atención a ello, atendiendo a los objetivos propuestos e hipótesis planteada, hemos comprobado su validez, puesto que: i) hemos comprobado que existen problemas de tipificación; ii) hay conductas que necesitan ser tipificadas como delitos; iii) hay confusión con algunos tipos penales; iv) hemos demostrado que hay un nuevo bien jurídico que necesita ser protegido.

9. CONCLUSIONES

1. Es correcto usar el término de criminalidad informática o tecnológica, cuando el agente utiliza los medios informáticos en la comisión de diversos delitos, no necesariamente o exclusivamente a los que se conocen como delitos informáticos.

2. La seguridad de la comunicación e información almacenada en medios informáticos, aparece como un nuevo bien jurídico nuevo merecedor de protección penal.

3. Es necesario la reforma integral del Código Penal para: i) adecuar las diversas conductas ilícitas a sus nuevas formas de comisión (con el uso de medios informáticos); ii) ampliar o corregir el objeto material o inmaterial de protección; iii) incluir nuevas conductas que afectan el nuevo bien jurídico; iv) las conductas punibles que utilizan sistemas informáticos y que vulneran el nuevo bien jurídico deben tipificarse como delitos de peligro.

4. La adecuación o reforma del Código Penal, así como la inclusión de nuevas conductas en el catálogo de ilícitos penales, debe propender a la unificación de conductas ilícitas típicas con otros países o atendiendo a

recomendaciones de organismos internacionales, de modo que pueda aplicarse la cooperación internacional.

10. RECOMENDACIONES

En atención a lo expuesto, consideramos necesario hacer la siguiente propuesta de lege ferenda:

a. **Necesidad de una propuesta legislativa integral.**

b. **Alcances de la Ley contra la Criminalidad Informática.**

c. **Los tipos penales.**

La propuesta se basa en las normas de organismos supranacionales la legislación comparada y la casuística de las modalidades que utilizan los delincuentes informáticos las cuales han sido obtenidas en el desarrollo de la presente investigación.

Aunque reconozco la imperiosa necesidad de legislar sobre aspectos procesales y se debe suscribir instrumentos supranacionales para enfrentar eficazmente la delincuencia informática la propuesta que presento no aborda esos aspectos por exceder los límites de esta tesis.

En la presente investigación he demostrado que las tecnologías de la información y comunicación pueden ser utilizadas como medio o afectan un nuevo bien jurídico de tal manera que se hace necesario adecuar algunos tipos penales a la nueva

realidad criminal y, respetando el principio de legalidad, sean aptos para combatirla como ha ocurrido con los tipos de pornografía infantil y turismo sexual de menores al incorporar los artículos 181-A y 183- A.

En los referido a la reforma del Código penal para hacerlo apto de enfrentarse a la criminalidad informática tenemos que comenzar por dictar una regla general que permita que se agrave la acción cuando el agente realice una acción típica utilizando medios informáticos o tecnológicos. De esta manera se reconoce que los medios tecnológicos pueden ser utilizados prácticamente para cometer cualquier conducta punible.

En los delitos contra el honor resulta conveniente incluir en la agravante la internet u otro medio de difusión masiva que ofrece las tecnologías de la información de la difamación que actualmente son ampliamente empelados en la comunicación y difusión de las ideas. De esta manera, se supera el concepto restrictivo del elemento normativo del tipo actual "medio de comunicación social" que puede excluir a las nuevas formas de comunicación que ofrece la tecnología.
Los delitos contra la intimidad y el secreto de las comunicaciones hay que ampliar el objeto material sobre el cual recae la conducta pues éstos han sido concebido teniendo en cuenta los medios clásicos de comunicación o registro que emplean al papel e integrar a cualquier forma de comunicación independiente del soporte o medio utilizado.

Los delitos contra la indemnidad sexual se realizó una primera adecuación a la realidad criminal que emplea medios tecnológicos con la inclusión de los artículos 181-A y 183- A sin embargo, este rubro necesita un ajuste que permita integrar todas las modalidades que aprovechan la tecnología.

En los delitos contra el patrimonio individual propongo mantener el tipo penal de transferencia ilegal electrónica de fondos o hurto telemático como una modalidad agravada del hurto debido a que esta conducta resulta apta para la persecución de esta actividad criminal. De hecho en la investigación realizada he constatado que la persecución penal en esta modalidad delictiva ha sido adecuada.

De otro lado, hay que reconocer que la criminalidad informática o tecnológica actúa de manera organizada y constituye un problema que debe ser enfrentado incluyendo como una conducta agravada del delito de asociación ilícita para delinquir.

En cuanto a los delitos contra la fe pública es conveniente integrar en el objeto material denominado "documento" a las nuevas formas de conservación y registro microforma, documento electrónico, certificado digital, documentos suscritos con firma digital, que ya se encuentran integradas a la legislación nacional como medio de conservación de datos, archivos oficiales y pueden ser utilizados como elementos probatorios en una controversia judicial.

La ***Ley contra la Criminalidad Informática*** que propongo debe enfrentar el problema de la criminalidad tecnológica de manera integral; sin embargo, para mantenerme en los alcances y objetivos de esta investigación, presento únicamente la derogatoria de la Ley Nº 27309 y la inclusión de nuevas conductas típicas que nos trae la nueva realidad delictiva. Empero, la Ley contra la Criminalidad Informática para que realmente sea un instrumento útil en la lucha contra la nueva delincuencia deberá abarcar dos secciones: i) dogmática, que comprende la reforma integral del Código Penal y la tipificación de las nuevas conductas que afectan el bien jurídico denominado datos ii) aspectos procesales en la cual se establezcan reglas que permitan, respetando los derechos fundamentales, vigilancia y la obtención de pruebas en el mundo virtual.

Esta ley se justifica por que conforme he demostrado en la presente investigación nos encontramos ante una nuevo bien jurídico ***"seguridad de los datos informáticamente procesados o almacenados"*** de carácter supraindividual que necesita ser protegido de diversos ataques que lo lesionen o lo pongan en peligro concreto.

Asimismo, por la importancia del nuevo bien jurídico se debe tipificar las conductas como tipos de peligro concreto y las penas deben incrementarse proporcionalmente a la lesión ocasionada.

En la Ley contra la Criminalidad Informática se consignan los siguientes tipos penales:

1. Accesos indebidos o sin autorización

2. La omisión de implementar medidas de seguridad. En esta conducta se considera garante al responsable o administrador de un sistema informático que sea el encargado de instalar y regular las medidas de seguridad. La conducta se justifica por la importancia del bien jurídico tutelado el cual es un bien jurídico colectivo.

Por ello, la propuesta de *lege ferenda* contiene dos secciones:

1. Modificaciones al Código Penal
2. Ley contra la Criminalidad Informática

Propuesta de lege ferenda.

1. **Modificaciones al Código Penal**

Agravante genérica.

Artículo 46-B Constituye circunstancia agravante de la responsabilidad penal si el sujeto activo utiliza, en la comisión del delito, sistema informático o la telemática en general cuando el uso de la informática no se encuentre expresamente indicada en la conducta punible.

En estos casos la pena se incrementará en un tercio por encima del límite legal fijado para el delito cometido sin exceder el máximo de pena privativa de libertad establecido en el artículo 29 del Código Penal.

DIFAMACIÓN

Artículo 132.- El que, ante varias personas, reunidas o separadas, pero de manera que pueda difundirse la noticia, atribuye a una persona, un hecho, una cualidad o una conducta que pueda perjudicar su honor o reputación, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a ciento veinte días-multa.

AGRAVANTE

Si la difamación se refiere al hecho previsto en el artículo 131º, la pena será privativa de libertad no menor de uno ni mayor de dos años con noventa a ciento veinte días-multa.

Si el delito se comete por medio del libro, la prensa u otro medio de comunicación ~~social~~ o la internet la pena será privativa de libertad no menor de tres ni mayor de seis años y de ciento veinte a trescientos sesenticinco días-multa.

Violación de la intimidad.

Artículo 154.- El que viola la intimidad de la vida personal observando, escuchando o registrando un hecho, palabra, escrito o imagen, empleando cualquier medio o procesos tecnológicos capaces de registrar, transmitir o almacenar información, será reprimido con pena privativa de libertad no menor de 02 ni mayor de 04 años.

La pena será no menor de 03 ni mayor de 06 años y de treinta a ciento veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista.

El que divulga a través de cual medio de comunicación o cualquier medio capaz de comunicar a dos o más personas, o publica en página web, red social o mediante la internet aspectos de la intimidad personal, la pena privativa de libertad será no menor de tres ni mayor de seis años y de sesenta a ciento ochenta días-multa.

Agravante: calidad del sujeto activo.

Artículo 155.- Si el agente es funcionario o servidor público y, en ejercicio del cargo, o es director o editor de un medio de comunicación o de un blog o página web comete el hecho previsto en el artículo 154º, la pena será no menor de tres ni mayor de 08 años e inhabilitación conforme al artículo 36º, incisos 1, 2 y 4.

Apoderamiento indebido del secreto de comunicaciones.

Artículo 161.- El que, indebidamente, se apodera, intercepta, suprime o extravía una carta, telegrama, radiograma o cualquier tipo de comunicación publicada en página web o red social, vía transferencia de datos, realizada por cualquier medio capaz de comunicar a dos o más personas o que se difunda mediante la internet, que se realice cualquier vía aunque no haya llegado a su destinatario será

reprimido con pena privativa de libertad no menor 02 ni mayor de 06 años y con sesenta a noventa días-multa.

La misma pena tendrá aquel que indebidamente acceda, copie o transfiera cualquier tipo de comunicación privada que se transmita o produzca en cualquier medio o sistema informático.

Interferencia de las comunicaciones.

Artículo 162.- El que, indebidamente, interfiere o escucha una conversación telefónica o realizada por cualquier medio tecnológico, correo electrónico, mensaje de voz o publicada en página web o red social, vía transferencia de datos, realizada por cualquier medio capaz de comunicar a dos o más personas, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

Si el agente es funcionario público, administrador o proveedor de un servicio de internet la pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitado conforme al artículo 36º, incisos 1, 2 y 4.

Publicación indebida de correspondencia.

Artículo 164.- El que publica, difunde o transmite indebidamente, una correspondencia epistolar o telegráfica, correo electrónico, o publicada en página web o red social, vía transferencia de datos, contenida en cualquier tipo de soporte, no destinada a la publicidad, aunque le haya sido dirigida, será reprimido, si el hecho causa algún perjuicio a otro, con limitación de días libres de veinte a cincuentidós jornadas.

Violación de la libertad de información

Artículo 169.- El funcionario público que, abusando de su cargo, suspende o clausura algún medio de comunicación social o página web, red social, vía

transferencia de datos, realizada por cualquier medio capaz de comunicar a dos o más personas que se difunda mediante la internet, o impide su circulación o difusión, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36º, incisos 1 y 2.

Artículo 181-A.- Turismo sexual infantil

El que promueve, publicita, favorece o facilita el turismo sexual, a través de cualquier medio escrito, folleto, impreso, visual, audible, electrónico, magnético o a través de internet o publicada en página web o red social, vía transferencia de datos, realizada por cualquier medio capaz de comunicar a dos o más personas que se difunda mediante la internet, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de catorce y menos de dieciocho años de edad será reprimido con pena privativa de libertad no menor de dos mi mayor de seis años.

Si la víctima es menor de catorce años, el agente, será reprimido con pena privativa de libertad no menor de seis ni mayor de ocho años.

El agente también será sancionado con inhabilitación conforme al artículo 36º incisos 1,2, 4 y 5.

Será no menor de ocho ni mayor de diez años de pena privativa de la libertad cuando ha sido cometido por autoridad pública, sus ascendientes, maestro o persona que ha tenido a su cuidado por cualquier título a la víctima.

Artículo 182º-A.- Publicación en los medios de comunicación sobre delitos de libertad sexual a menores.

Los gerentes o responsables de las publicaciones o ediciones a transmitirse a través de los medios de comunicación masivos, o publicada en página web o red social, vía transferencia de datos o que se difunda mediante la internet o cualquier medio de transmitir información o por cualquier medio capaz de comunicar a dos o más

personas que publiciten la prostitución infantil, el turismo sexual infantil o la trata de menores de dieciocho años de edad serán reprimidos con pena privativa de la libertad no menor de dos ni mayor de seis años.

El agente también será sancionado con inhabilitación conforme al inciso 4 del artículo 36º y con trescientos sesenta días multa.

Artículo 183º.- Exhibiciones y publicaciones obscenas

Será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años el que, en transmite a través de cualquier medio, o publicada en página web o red social, vía transferencia de datos, realizada por cualquier medio capaz de comunicar a dos o más personas que se difunda mediante la Internet o cualquier medio de transmitir información, lugar público, realiza exhibiciones, gestos, tocamientos u otra conducta de índole obscena.

Agravante.

Será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años:

1. El que muestra, vende o entrega a un menor de dieciocho años, por cualquier medio, o publicada en página web o red social, vía transferencia de datos, realizada por cualquier medio capaz de comunicar a dos o más personas que se difunda mediante la internet, incluyendo la internet, objetos, libros, escritos, imágenes, visuales o auditivas, que por su carácter obsceno, pueden afectar gravemente el pudor, excitar prematuramente o pervertir su instinto sexual.
2. El que incita a un menor de dieciocho años a la práctica de un acto obsceno o le facilita la entrada a los prostíbulos u otros lugares de corrupción.

3. El administrador, vigilante o persona autorizada para controlar un cine u otro espectáculo donde se exhiban representaciones obscenas, que permita ingresar a un menor de dieciocho años.

La misma pena tendrá el que solicite a un menor que exponga las partes íntimas de su cuerpo a través de la internet o red social,

Artículo 183º A.- Pornografía Infantil

El que produce, elabora, posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio tecnológico, sistema de información o tecnología de información o incluido la internet, objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, o publica en página web o red social, vía transferencia de datos, realizada por cualquier medio capaz de comunicar a dos o más personas que se difunda mediante la internet, o las difunde a través de la internet o las mantenga en una base de datos o en cualquier tipo de soporte que grabe o reproduzca imágenes o video, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de 08 años y con ciento veinte a trescientos días multa.

Cuando se utilice a un menor de catorce años de edad la pena será no menor de 08 ni mayor de 12 años y con ciento cincuenta a trescientos sesenta y cinco días multa.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173º, o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil la pena privativa de libertad será no menor de 12 ni mayor de 16 años.

De ser el caso, el agente será inhabilitado conforme al artículo 36º, incisos 1, 2, 4 y 5.

A efectos de este artículo se entenderá "pornografía infantil" cualquier material que contenga la representación visual de :

1. un menor adoptando un comportamiento sexualmente explícito;
2. una persona que parezca un menor adoptando un comportamiento sexualmente explicito;
3. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

Hurto informático

Artículo 186.- El agente será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años si el hurto es cometido:

1. En casa habitada.
2. Durante la noche.
3. Mediante destreza, escalamiento, destrucción o rotura de obstáculos.
4. Con ocasión de incendio, inundación, naufragio, calamidad pública o desgracia particular del agraviado.
5. Sobre los bienes muebles que forman el equipaje de viajero.
6. Mediante el concurso de dos o más personas.

La pena será no menor de cuatro ni mayor de ocho años si el hurto es cometido:

1. Por un agente que actúa en calidad de integrante de una organización destinada a perpetrar estos delitos.
2. Sobre bienes de valor científico o que integren el patrimonio cultural de la Nación.
3. Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o empleando claves secretas.

4. Colocando a la víctima o a su familia en grave situación económica.
5. Con empleo de materiales o artefactos explosivos para la destrucción o rotura de obstáculos.
6. Utilizando el espectro radioeléctrico para la transmisión de señales de telecomunicación ilegales.

La pena será no menor de ocho ni mayor de quince años cuando el agente actúa en calidad de jefe, cabecilla o dirigente de una organización destinada a perpetrar estos delitos.

APROPIACIÓN DE BIEN PERDIDO O TESORO

Artículo 192.- Será reprimido con pena privativa de libertad no mayor de dos años o con limitación de días libres de diez a veinte jornadas, quien realiza cualquiera de las acciones siguientes:

1. Se apropia de un bien que encuentra perdido o de un tesoro o de la parte del tesoro correspondiente al propietario del suelo, sin observar las normas del Código Civil.
2. Se apropia de un bien ajeno en cuya tenencia haya entrado a consecuencia de un error, caso fortuito o por cualquier otro motivo independiente de su voluntad.

La pena será no menor de dos años ni mayor de seis años si se apropia de medios electrónicos de pago

196 – A Fraude informático REVISAR

El que, utilizando cualquier elemento informatico o medio tecnológico para alterar la información almacenada en un sistema de información con el objeto de obtener

un beneficio patrimonial ilícito será reprimido con pena privativa de la libertad no menor de 02 a 08 años

Artículo 317º.- Asociación ilícita.

El que forma parte de una organización de dos o más personas destinada a cometer delitos será reprimido por el sólo hecho de ser miembro de la misma, con pena privativa de libertad no menor de tres ni mayor de seis años.

Cuando la organización esté destinada a cometer los delitos previstos en los artículos … y los contemplados en la Ley Nº … Ley contra la Criminalidad Informática, 152º al 153º-A, 200º, 273º al 279º-D, 296º al 298º, 315º, 317º, 318º-A, 319º, 325º al 333º; 346º al 350º o la Ley Nº 27765 (Ley Penal contra el Lavado de Activos), la pena será no menor de ocho ni mayor de quince años, de ciento ochenta a trescientos sesenta y cinco días-multa e inhabilitación conforme al artículo 36º incisos 1, 2 y 4, imponiéndose además, de ser el caso, las consecuencias accesorias del artículo 105º numerales 2) y 4), debiéndose dictar las medidas cautelares que correspondan para garantizar dicho fin.

FALSEDAD DOCUMENTAL

Artículo 427.- El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho, con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años y con treinta a noventa días-multa si se trata de un documento público, registro público, microforma, documento electrónico, certificado digital, documentos suscritos con firma digital, título auténtico o cualquier otro transmisible por endoso o al portador y con pena privativa de libertad no menor de dos ni mayor de cuatro años, y con ciento ochenta a trescientos sesenticinco días-multa, si se trata de un documento privado.

El que hace uso de un documento falso o falsificado, como si fuese legítimo, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas.

EQUIPARACION A DOCUMENTO PÚBLICO

Artículo 433.- Para los efectos de este Capítulo se equiparan a documento público, los testamento ológrafo y cerrado, los títulos-valores, los títulos de crédito transmisibles por endoso o al portador y las microformas, los documentos electrónicos, certificados digitales o documentos suscritos con firma digital.

FALSEDAD GENERICA

Artículo 438.- El que de cualquier otro modo que no esté especificado en los Capítulos precedentes, comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos, o usurpando nombre, calidad o empleo que no le corresponde, o utilizando información personal obtenida con medios informáticos, suponiendo viva a una persona fallecida o que no ha existido, o viceversa, será, será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años.

La pena será no menor de cuatro ni mayor de ocho años si el agente obtiene un beneficio económico o utiliza medios informáticos o tecnológicos.

2. **Ley contra la Criminalidad Informática.**

DAÑOS INFORMATICOS

El que destruya, dañe, borre, deteriore, altere, inutilice o suprima datos informáticos, o un sistema de tratamiento de información o medios semejantes alguna de sus partes o componentes lógicos, será reprimido con pena privativa de libertad no menor de 04 ni mayor de 06 años y con prestación de servicios comunitarios de ciento cincuentidós a trescientas jornadas.

APROPIACIÓN DE MEDIO ELECTRÓNICO DE PAGO.

El que indebidamente se apropia de un medio electrónico de pago será reprimido con pena privativa de libertad no menor de cuatro años ni menor de seis años.

La misma pena se impondrá a quien, indebidamente, adquiere, recibe, usa o transporta el medio electrónico de pago.

POSESION INDEBIDA DE MEDIOS O EQUIPOS PARA FABRICAR MEDIOS DE PAGO.

El que, indebidamente, recibe, adquiere, posee, transporta, distribuye, entrega, comercializa, por cualquier medio, programas o equipos para fabricar medios de pago o componentes de estos medios de pago o equipos que permitan copiar medios de pago será reprimido con pena privativa de libertad no menor de cuatro años ni menor de seis años.

ACCESO INDEBIDO

El que, sin autorización, accede, intercepte o utiliza en todo o en parte a un sistema de informático, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será reprimido con pena privativa de libertad no menor de 02 ni mayor de 05 años y con prestación de servicios comunitarios de ciento cincuentidós a trescientas jornadas.

Responsabilidad por omisión de implementación de medidas de seguridad

El responsable de una base de datos, que conserve información sensible, pública o de una entidad bancaria o financiera, que no cumpla con implementar medidas de seguridad para evitar la instalación de programas maliciosos o perjudiciales será reprimido con pena privativa de libertad no menor de dos años mayor de 6 años

Elaboración o Comercialización de bases de datos

El que, sin autorización, elabore, ofrezca, venda, transfiera, envíe, difunda, suba a la red o…. una base de datos que contenga información de carácter personal que se encuentre contenida en medios informáticos o soporte de información o medios telemáticos o semejantes será reprimido con pena privativa de libertad no menor de dos ni mayor de seis.

MANEJO FRAUDULENTO DE MEDIOS ELECTRONICOS DE PAGO

Será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años, el que, sin autorización, realice cualquiera de las siguientes conductas:

1. Cree, capture, grabe, copie, altere, duplique o elimine por cualquier medio la data o información contenidas en un medio electrónico de pago.
2. Cree, duplique o altere mediante el uso de tecnologías de información, la data o información en un sistema de información con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos.
3. Adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de medios electrónicos de pago o de la data o información contenidos en ellos o en un sistema de información.

SUPLANTACIÓN DE SITIOS WEB.

El que, sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, será sancionado con pena privativa de libertad no menor de 02 ni mayor de 08 años

La misma pena corresponderá al que utilice el nombre de dominio de otro e induzca a los usuarios a ingresar a una IP diferente.

OBSTACULIZACIÓN DEL SISTEMA INFORMATICO

El que, indebidamente, impida, dificulte u obstaculice el funcionamiento o el acceso a un sistema informático o a los datos informáticos allí contenidos, o a una red de telecomunicaciones, mediante la transmisión, introducción, daño deterioro, alteración o supresión de datos informáticos.

La misma pena se impondrá a quien copia, captura, graba, copia, trasmite, difunde data o información contenida en cualquier medio de pago.

AGRAVANTES

En los casos de los artículos …….. la pena será privativa de libertad no menor de cuatro ni mayor de diez años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, o utilizando su código de acceso, obtenida en función a su cargo.

2. El agente afecta o accede a una base de datos o página web de un servicio público o de una institución estatal o pone en peligro la seguridad nacional.

3. El agente accede a un sistema de información que contenga información financiera, bancaria, económica o sobre procesos tecnológicos,

4. El agente utiliza virus informático o programa malicioso capaz de transmitirse por la red o otros sistemas informáticos.

5. El agente propaga un virus o programa malicioso que cause un perjuicio económico.

Normas derogatorias

Derógase los artículos 207 – A, 207 – B y 207 – C, promulgados por Ley Nº 27309.

11. BIBLIOGRAFÍA

1. ALVAREZ-CIENFUEGOS SOTO, José. Los delitos relativos a la informática. En: El Código Penal de 1995: Parte especial. Consejo General del Poder Judicial. Barcelona.
2. ANTOLISEI, Francesco. Problema del bene giurídico. En: Rivista Italiana di Diritto Penale, Edit. Giuffre, Milano, 1939.
3. BACIGALUPO ZAPATER, Enrique. Derecho Penal – Parte General. Ed. ARA. Lima 2004.
4. BACIGALUPO ZAPATER, Enrique. Utilización abusiva de cajeros automáticos por terceros no autorizados. En: Jornadas de estudio sobre nuevas formas de delincuencia. Centro de Estudios Judiciales. Madrid. 1988.
5. BAJO FERNÁNDEZ, Miguel. Manual de Derecho Penal, Parte Especial (Delitos patrimoniales y económicos) Ed. Centro de Estudios Ramón Areces. Madrid. 1989.
6. BERDUGO GÓMEZ DE LA TORRE, Ignacio. Lecciones de Derecho Penal – Parte General. Ed. Praxis. Barcelona – España 1999.
7. BERDUGO GÓMEZ de la Torre, Ignacio. Honor y Libertad de expresión. Editorial TECNOS, 1987, Madrid – España.
8. BERNALES BALLESTEROS, Enrique. La Constitución de 1993. Análisis comparado, Ed. RAO, 5ª. Ed. Lima 1999.

9. Bettiol, Giuseppe. Instituzioni di diritto e procedura penale. Principi Fondamentali del Diritto penale vigente, terza edizione, Padova. Cedam. Casa Editrice, Bolonia, 1984.

10. BOIX REIG, Javier. Protección jurídico-penal de la intimidad y la informática. En: Jornadas de estudio sobre nuevas formas de delincuencia. Centro de Estudios Judiciales. Madrid. 1988.

11. BRAMONT-ARIAS TORRES, Luis Alberto y GARCIA CANTIZANO, María del Carmen. Manual de Derecho Penal. Parte Especial. San Marcos. Lima 1998.

12. BRAMONT-ARIAS TORRES, Luis. El delito informático en el Código Penal Peruano. PUCP Fondo Editorial. Lima. 1997.

13. BRAMONT-ARIAS TORRES, Luis. El delito informático. (Ley Nº 27309, de 17 de julio del 200) En: Gaceta Jurídica. Tomo 81-B agosto, 2000.

14. BUENO ARÚS, Francisco. El delito informático. En Actualidad informática Aranzandi. Nº 11. Abril de 1994

15. BUENO ARÚS, Francisco. Los delitos relativos a la informática. En: El Código Penal de 1995: Parte especial. Consejo General del Poder Judicial. Barcelona.

16. BUITRAGO RUIZ, Ángela. El delito informático. En: Derecho Penal y Criminología. Revista del Instituto de Ciencias Penales y Criminológicas. Volumen XVIII. Número 59. Mayo/Agosto 1996.

17. BUSTOS RAMÍREZ, Juan. Manual de Derecho Penal – Parte General. Ed. Ariel. 3ª. Edición. Barcelona 1993.

18. BUSTOS RAMÍREZ, Juan. Los bienes jurídicos colectivos: control social y sistema penal. PPU. Barcelona 1987.

19. CÁCERES J., Roberto y otro. Código Procesal Penal Comentado, Jurista Editores, Lima 2006.

20. CARPIO MARCOS, Edgar. La interpretación de los derechos fundamentales. Palestra Editores. 1ª. Edición. Lima, enero 2004.

21. CARRIO, Alejandro. Garantías constitucionales en el proceso penal. Ed. Hammurabi. 3ª. Edición, 1ª. Reimpresión 1997. Buenos Aires – Argentina.

22. CASTILLO ALVA, José Luis. Principios de Derecho Penal – Parte General. Ed. Gaceta Jurídica. Lima 2002.

23. CASTILLO ALVA, José Luis (Coordinador). Código Penal comentado. Ed. Gaceta Jurídica. Lima 2004.

24. CASTILLO ALVA, José Luis. Algunas consideraciones sobre el bien jurídico en los delitos contra el patrimonio. En: Revista Peruana de Ciencias Penales. Edición especial sobre el Código Penal peruano. N° 11.

25. CEREZO MIR, José. Curso de Derecho penal español – Parte General. Ed. Tecnos. 6ª. Edición. Madrid 2004.

26. COBO DEL ROSAL, Manuel y VIVES ANTÓN. *Derecho penal. Parte general*, Edit. Tirant lo Blanch, Madrid, 1988.

27. CONDE PUMPIDO, Cándido. Las tarjetas de crédito como instrumento para la comisión de un delito: dos sentencias. En: Jornadas de estudio sobre nuevas formas de delincuencia. Centro de Estudios Judiciales. Madrid. 1988.

28. CORCOY BIDASOLO, Mirentxu. Protección Penal del sabotaje informático. Especial consideración de los delitos de daños. En: Delincuencia Informática. PPU, Barcelona, 1992.

29. CORCOY BIDASOLO, Mirentxu. Legislación Penal sobre protección de la criminalidad en distintos países europeos. En: Delincuencia Informática. PPU, Barcelona, 1992.

30. CORCOY BIDASOLO, Mirentxu. Delitos de peligro y protección de bienes jurídicos supraindividuales. Tirant lo blach, Valencia. 1999.

31. CHOCANO RODRÍGUEZ, Reiner. La falsedad documental del artículo 427 del CP. En: Revista Peruana de Doctrina y Jurisprudencia Penal, IPCC, Grijley, Lima, 2000.

32. DAVARA RODRIGUEZ, Miguel. Las autopistas de la información y los profesionales del Derecho. En: Actualidad informática Aranzandi. Nº 21. Octubre de 1996.

33. DAVARA RODRIGUEZ, Miguel. El Documento electrónico, informático y telemático y la firma electrónica. En: Actualidad informática Aranzandi. Nº 24. Julio de 1997

34. DE ASÍS ROIG, Rafael. Escritos sobre Derechos Humanos. ARA Editores. 1ª. Edición. Lima 2005.

35. DE LA HIZ MATÍAS, Juan José y CARRASCOSA LÓPEZ, Valentín. Estafa Informática. En: Informática y Derecho. Número 12-14. UNED. Mérida.

36. DOMAICA MAROTO, Juana María. El fraude Informático. ¿Un riesgo asegurable? En: Actualidad Jurídica Aranzandi. Editorial Aranzandi.

37. GARCÍA CANTIZANO, María del Carmen. Falsedades Documentales. Tirant lo blanch, Valencia, 1994.

38. GARCÍA CANTIZANO, María del Carmen. Falsedades Documentales. (En el Código Penal de 1995). Tirant lo blanch, Valencia, 1997.

39. GARCÍA CANTIZANO, María. La delincuencia informática en el ordenamiento jurídico peruano. En: Gaceta Jurídica. Tomo 78-B, Mayo 2000.

40. GIL MARTÍNEZ, Antonio. Algunos supuestos delictivos de tarjetas de crédito y cajeros automáticos. En: Jornadas de estudio sobre nuevas formas de delincuencia. Centro de Estudios Judiciales. Madrid. 1988.

41. GONZALES RUS, Juan José. Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos. En: Jornadas de estudio sobre nuevas formas de delincuencia. Centro de Estudios Judiciales. Madrid. 1988.

42. GONZALES RUS, Juan José. Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos. En: Informática y Derecho. Revista de la Facultad de Derecho de la Universidad Complutense. Número 12. Madrid. 1986

43. GUIBOURG, Ricardo y otros. Manual de Informática jurídica. Ed. Astrea. Bs. As.

44. GUTIÉRREZ FRANCÉS, María Luz. Fraude informático y estafa (Aptitud del tipo de estafa en el Derecho Español ante las defraudaciones por medios informáticos) Ministerio de Justicia. Secretaría Técnica. Centro de Publicaciones. Madrid. 1991.

45. GUTIÉRREZ FRANCÉS, María Luz. Delincuencia Económica e informática en el Nuevo Código Penal. Notas sobre la Delincuencia Informática: Atentados contra la "información" como valor económico de la empresa. En: Estudios de Derecho Penal Económico. Ed. de la Universidad de Castilla-La Mancha. 1994.

46. GUTIÉRREZ FRANCÉS, María Luz. En torno a los fraudes Informáticos en el Derecho español. En: Actualidad informática Aranzandi. Nº 11. Abril de 1994.

47. GUTIÉRREZ FRANCÉS, María Luz. Los fraudes informáticos en el nuevo Código Penal. En: Los delitos relativos a la informática. En: El Código Penal de 1995: Parte especial. Consejo General del Poder Judicial. Barcelona.

48. HASSEMER, Winfried. Fundamentos de Derecho Penal. Ed. Bosch. Barcelona 1984.

49. HERRERO HERRERO, César. Modelos peculiares de estafa. Estafa con tarjetas de crédito con y sin banda magnética. Estafas por medio del ordenador. Boletín Nº 1701. Secretaría General Técnica. Madrid.

50. HUERTA GUERRERO, Luis Alberto. El debido proceso en las decisiones de la Corte Interamericana de Derechos Humanos. Comisión Andina de Juristas. Lima, octubre de 2003.

51. HUERTA M. Marcelo y LIBANO M. Claudio. Delitos informáticos. 2da Edición. Ed. Jurídica Cono Sur Ltda. Stgo. de Chile. 1998.

52. HURTADO POZO, José. Manual de Derecho Penal – Parte General. Ed. Grijley. Lima 2005.

53. JAÉN VALLEJO, Manuel. Justicia penal contemporánea. Ed. Portocarrero. 1ª. Edición. Lima, agosto de 2002.

54. JESCHECK, Hans-Heinrich. Tratado de Derecho Penal – Parte General. Trad. Manzanares, Samaniego, Comares. Ed. Granada, 2002. España.

55. Laurenzo Copello, Patricia. El bien jurídico en los delitos contra el honor, en Revista Peruana de Ciencias Penales Nº 12.

56. LIBANO MANZUR, Claudio. Chile: Los delitos de Hacking en sus diversas manifestaciones. En: Revista Electrónica de Derecho Informático. http:// www. publicaciones.derecho.org/redi/ Nº 09. Abril del 2000.

57. LUZÓN PEÑA, Diego-Manuel. Curso de Derecho Penal – Parte General. Ed. Universitas. Madrid 1996.

58. MARTINEZ-BUJAN PEREZ. Derecho Penal Económico. Valencia 1998.

59. Mazuelos, Julio. Delitos informáticos: Una aproximación a la regulación del CP peruano. En: Revista Peruana de Doctrina y Jurisprudencia Penales. N° 2. 2001. Ed. Grijley

60. MEZGER, Edmund. Tratado de Derecho Penal. Trad. José Rodríguez. Ed. Revista de Derecho Privado. Madrid 1955.

61. MIR PUIG, Santiago. Derecho Penal – Parte General. 4ª. Ed., PPU, Barcelona 1995.

62. MIR PUIG, Santiago. (Comp) Delincuencia Informática. PPU, Barcelona, 1992.

63. MOHRENSCHLAGER, Manfred. Tendencias de la política jurídica en la lucha contra la delincuencia relacionada con la informática. En: Delincuencia Informática. PPU, Barcelona, 1992.

64. MOHRENSCHLAGER, Manfred. El nuevo Derecho Penal informático en Alemania. En: Delincuencia Informática. PPU, Barcelona, 1992.

65. MORÓN LERMA, Esther. Internet y Derecho Penal: "Hacking" y otras conductas ilícitas en la Red. Ed. Aranzandi. Pamplona. 1999.

66. MUÑOZ CONDE, Francisco. Derecho Penal – Parte Especial. Ed. Tirant lo Blanch. 16ª. Edición. Valencia – España 2007.

67. MUÑOZ CONDE, Francisco / GARCÍA ARÁN, Mercedes. Derecho Penal Parte General, Madrid. S.f.e.

68. ORTS BERENGUER, Enrique y otros. Derecho Penal, Parte Especial. 2da Ed. p. 654. Ed. Tirant lo Blanch. Valencia. 1996.

69. PÉREZ LUÑO, Antonio. Manual de Informática y Derecho. Ariel Derecho. Barcelona.

70. PESO NAVARRO, Emilio. La seguridad de la información. En: Actualidad informática Aranzandi. Nº 24. Julio de 1997

71. PISAPIA, Gian Doménico. Instituzioni di Diritto Penale. Parte Generale e Parte Speciale, Padova. Cedam. Casa editricce. Dott, Vicenza, 1965.

72. PUERTA LUIS, Luis. Las tarjetas de crédito en el campo penal. En: Jornadas de estudio sobre nuevas formas de delincuencia. Centro de Estudios Judiciales. Madrid. 1988.

73. REYNA ALFARO, Luis Miguel. Los delitos informáticos. Jurista Editores. Lima, enero 2002.

74. ROJAS VARGAS, Fidel. Estudios de Derecho Penal _ Doctrina y Jurisprudencia. Jurista Editores. 1ª. Edición. Julio 2004. Lima – Perú.

75. ROJAS VARGAS, Fidel; et allie. Código Penal. Catorce años de jurisprudencia sistematizada. Ed. Idemsa. Lima 2001.

76. ROJAS VARGAS, Fidel. Delitos contra el patrimonio. Vol I. Grijley. Lima 2000.

77. ROMEO CASABONA, Carlos. Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos. En: Jornadas de estudio sobre nuevas formas de delincuencia. Centro de Estudios Judiciales. Madrid. 1988.

78. ROMEO CASABONA, Carlos. Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías. En: Poder Judicial. Número 31. Setiembre 1993.

79. ROSALES ARTICA, David. El delito de falsificación de documentos. En: Revista Actualidad Jurídica No.160, Gaceta Jurídica, Lima marzo 2007.

80. ROXIN, Claus. Derecho Penal – Parte General. Trad. Luzón Peña, Díaz y García Conlledo, y De Vicente Remesal. Ed. Civitas. Madrid 1997.

81. ROXIN, Claus. La teoría del delito en la discusión actual. Trad. Manuel Abanto Vásquez. Ed. Grijley. Lima 2007.

82. ROXIN, Claus, et allie. Derecho Penal y Derecho Penal Procesal. Ed. Ariel. 1ª. Edición. España, marzo de 1989.

83. ROXIN, Claus. Código Penal alemán. StGB. Ed. Marcial Pons, 2000.

84. ROY FREYRE, Luis E. Derecho Penal Peruano. Parte Especial. Tomo III. IPCP, Lima 1983.

85. SALGADO CARMONA, Concepción. Delitos contra el honor. En: Cobo del Rosal, Manuel (Dir): Curso de Derecho penal español - Parte especial I, Marcial Pons, Madrid, 1996.

86. SIEBER, Ulrich. IUS Informationis. The Internacional Emergence of Criminal Information Law.

87. SILVA SÁNCHEZ, J.M. Aproximación al Derecho Penal Contemporáneo, Barcelona, 1992.

88. Schopenhauer, Arthur. La Sabiduría de la Vida, en torno a la filosofía. Editorial Porrúa, S.A. 2da. Edición, México 1991.

89. SCHUNEMANN, Bernd. Cuestiones básicas del Derecho Penal en los umbrales del tercer milenio. Trad. Mariana Sacher. Ed. Idemsa. Lima 2006.

90. TIEDEMANN, Klaus. Constitución y Derecho Penal. Palestra Editores. 1ª. Edición, Lima 2003.

91. TIEDEMANN, Klaus. Criminalidad mediante computadoras. En: Poder Económico y Delito. Ariel Derecho. Barcelona. 1985.

92. TIEDEMANN, Klaus. Criminalidad informática y derecho Penal. En: Derecho Penal y Nuevas formas de criminalidad. Traducción y edición de Manuel Abanto Vásquez. Idemsa. Lima, 2000.

93. URQUIZO OLAECHEA, José. El Bien Jurídico en Revista Peruana de Ciencias Penales, Nº 6.

94. URQUIZO OLAECHEA, José. Los delitos contra el honor en el nuevo Código Penal. En: RPCP Nº 1, Lima 1993.

95. VIEGA RODRÍGUEZ, María José. Delito Informático. En: Revista Electrónica de Derecho Informático. http:// www. publicaciones.derecho.org/redi/ Nº 09. Abril de 1999.

96. VILLAVICENCIO TERREROS, Felipe. Derecho Penal – Parte General. Ed. Grijley. Lima 2006.

97. VILLALBA DÍAZ, Federico. Los delitos y contravenciones informáticas. Los hackers y el Código Penal. En: Revista Electrónica de Derecho Informático. http:// www. publicaciones.derecho.org/redi/ Nº 09. Abril de 1999.

98. WESSELS, Johannes. Derecho Penal – Parte General. Trad. Conrado Finzi. Ed. Depalma. Buenos Aires 1980.

99. ZABALE, Ezequiel. Argentina: Pornografía, racismo e internet. En REDI Nº 22, mayo del 2000.

100. ZAFFARONI, Raúl. Tratado de Derecho Penal. Ed. Ediar. Buenos Aires 1982.